VERSITRON®

Your Copper to Fiber Connection

SG71660MA
Layer 2 Managed
16-Port 10/100/1000 Switch
with (4) 1000Base SFP Slots

User's Manual

© June 2011

VERSITRON, Inc.
83 Albe Drive – Suite C
Newark, DE 19702
www.versitron.com

PROPRIETARY DATA

All data in this manual is proprietary and may not be disclosed,
used or duplicated, for procurement or manufacturing purposes,
without prior written permission by **VERSITRON**.

VERSITRON LIFETIME WARRANTY

All VERSITRON products are covered by a **Lifetime Warranty** against defects in materials and workmanship. This coverage is applicable to the original purchaser and is not transferable.

We repair, or at our option, replace parts/products that, during normal usage and operation, are proven to be defective during the time you own the products, provided that said products and parts are still manufactured and/or available. Such repair/replacement is subsequent to receipt of your product at our facility and our diagnostic evaluation and review of the unit. **Advance replacements are not provided as part of the warranty coverage.**

This warranty does not cover damage to products caused by misuse, mishandling, power surges, accident, improper installation, neglect, alteration, improper maintenance, or other causes which are not normal and customary applications of the products and for which they were not intended. No other warranty is expressed or implied, and VERSITRON is not liable for direct, indirect, incidental or consequential damages or losses.

In the unlikely event a warranty issue should arise, simply contact us at 302-894-0699 or 1-800-537-2296 or via email at fiberlink@versitron.com to obtain a Return Material Authorization (RMA) number, along with instructions for returning your product.

Note: This warranty is effective for commercial products as of January 1, 2001 and for GSA products as of July 1, 2006.

Table of Contents

CAUTION VI
ELECTRONIC EMISSION NOTICES VI

1. INTRODUCTION 2

1-1. OVERVIEW OF SG71660MA MANAGED SWITCH 2
1-2. CHECKLIST 4
1-3. FEATURES 4
1-4. FULL VIEW OF THE SG71660MA 6
1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs) 6
1-4-2. AC Power Input on the Rear Panel 7
1-5. VIEW OF THE OPTIONAL MODULES 8

2. INSTALLATION 9

2-1. STARTING THE SG71660MA 9
2-1-1. Hardware and Cable Installation 9
2-1-2. Installing the SG71660MA into 19-Inch Wiring Closet Rail 11
2-1-3. Cabling Requirements 12
2-1-3-1. Cabling Requirements for TP Ports 12
2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module 12
2-1-3-3. Switch Cascading in Topology 13
2-1-4. Configuring the Management Agent of the SG71660MA 16
2-1-4-1. Configuring the Management Agent of SG71660MA through the Serial RS-232 Port 16
2-1-5. IP Address Assignment 19
2-2. TYPICAL APPLICATIONS 24

3. OPERATION OF WEB-BASED MANAGEMENT 26

3-1. WEB MANAGEMENT HOME OVERVIEW 28
3-1-1. System Information 31
3-1-2. Account Configuration 33
3-1-3. Time Configuration 34
3-1-4. IP Configuration 37
3-1-5. Loop Detection 40
3-1-6. Management Policy 41
3-1-7. System Log 44
3-2. PORT CONFIGURATION 45
3-2-1. Port Configuration 45
3-2-2.Port Status 47
3-2-3. Simple Counter 50
3-2-4. Detail Counter 52
3-3. VLAN 55
3-3-1. VLAN Mode 55
3-3-2. Tag-based Group 56
3-3-3. Port-based Group 58
3-3-4. Ports 60
3-3-5. Management 62
3-4. MAC 63
3-4-1. Mac Address Table 63
3-4-2. Static Filter 65
3-4-3. Static Forward 66
3-4-4. MAC Alias 67
3-4-5. MAC Table 68
3-5. GVRP 69
3-5-1. Config 69
3-5-2. Counter 72
3-5-3. Group 74
3-6. QOS(QUALITY OF SERVICE) CONFIGURATION 75
3-6-1. Ports 75
3-6-2. Qos Control List 77

3-6-3.Rate Limiters *82*
3-6-4.Storm Control *84*
3-6-5.Wizard *85*
3-7. SNMP CONFIGURATION 94
3-8. ACL 96
3-8-1.Ports *96*
3-8-2.Rate Limiters *98*
3-8-3.Access Control List *99*
3-8-4.Wizard *125*
3-9. IP MAC BINDING 133
3-10. 802.1X CONFIGURATION 135
3-10-1.Server *139*
3-10-2.Port Configuration *141*
3-10-3.Status *143*
3-10-4. Statistics *144*
3-11. TRUNKING CONFIGURATION 145
3-11-1.Port *146*
3-11-2 Aggregator View *148*
3-11-3 LACP System Priority *149*
3-12 STP CONFIGURATION 150
3-12-1 STP Status *150*
3-12-2. Configuration *152*
3-12-3. STP Port Configuration *154*
3-13 MSTP 156
3-13-1 Status *156*
3-13-2 Region Config *157*
3-13-3 Instance View *158*
3-14. MIRROR 165
3-15. IGMP SNOOPING 166
3-15-1 Proxy *166*
3-15-2 Group Membership *168*
3-16. ALARM CONFIGURATION 169
3-16-1 Events *170*
3-16-2 Email *171*
3-17. CONFIGURATION 172
3-17-1. Factory Defaults *172*
3-17-2 . Save Start *173*
3-17-3 . Save User *173*
3-17-4 . Restore User *173*
3-18. CONFIG FILE 174
3-19. DIAGNOSTICS 175
3-19-1 . Diagnostics *175*
3-19-2 .Ping *176*
3-19-2 .VeriPHY *177*
3-20 MAINTENANCE 177
3-20-1 .Reset Device *178*
3-20-2 .Software Upload *178*
3-21 LOGOUT 179

4. OPERATION OF CLI MANAGEMENT 180

4-1. CLI MANAGEMENT 180
4-1-1. Login *180*
4-2. COMMANDS OF CLI 182
4-2-1. Global Commands of CLI *183*
4-2-2. Local Commands of CLI *189*

5. MAINTENANCE 292

5-1. RESOLVING NO LINK CONDITION 292
5-2. Q&A 292

APPENDIX A TECHNICAL SPECIFICATIONS 293

APPENDIX B NULL MODEM CABLE SPECIFICATIONS.....297

Revision History

Release	Date	Revision
1.75	06/18/2011	A8

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

his equipment has been tested and found to comply with the protection requirements of European Emission Standard **EN55022/EN61000-3** and the Generic European Immunity Standard EN55024.
EMC:

EN55022(2003)/CISPR-2(2002)	class A
IEC61000-4-2 (2001)	4K V CD, 8KV, AD
IEC61000-4-3(2002)	3V/m
IEC61000-4-4(2001)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the SG71660MA through the built-in CLI and web by RS-232 serial interface and Ethernet ports step-by-step. Many explanation in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and command-line interface (CLI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of SG71660MA
- Chapter 2 "Installation"
- Chapter 3 "Operation of Web-based Management"
- Chapter 4 "Operation of CLI Management"
- Chapter 5 "Maintenance"

1. Introduction

1-1. Overview of the SG71660MA Managed Switch

The SG71660MA is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch features (12) 10/100/1000Mbps Twisted Pair (TP) ports and (4) Gigabit TP/SFP combo ports. The switch can be managed through the RS-232 serial port, or through an Ethernet port using CLI or Web-based management, associated with an SNMP agent. With the SNMP agent, the network administrator can logon to the switch to monitor, configure and control each port's activity. The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful functions such as ACL, IP-MAC Binding, DHCP Option 82, QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, and IGMP Snooping. It is suitable for both metro-LAN and office applications.

In this switch, Port 13 through Port 16 include two types of media --- TP and SFP Fiber; these ports support either 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detect function. 1000Mbps SFP Fiber transceivers are used for high-speed connection expansion.

The 10/100/1000Mbps TP ports are standard Ethernet ports that meet all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The 1000Mbps SFP Fiber ports are Gigabit Ethernet ports that fully comply with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceivers are designed with an optic Wavelength Division Multiplexing (WDM) technology that transport bi-directional full duplex signals over a single fiber simultaneously.

For upgrading firmware, please refer to the Section 3-21 or Section 4-2-2 for more details. The switch will not stop operating while upgrading the firmware and after that, the configuration remains unchanged.

• Key Features in the Device

QoS:

Supports Quality of Service by the IEEE 802.1P standard. There are two priority queues and packet transmission schedule.

Spanning Tree:

Supports IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

VLAN:

Supports Port-based VLAN and IEEE802.1Q Tag VLAN. Supports 256 active VLANs and VLAN ID 1~4094.

Port Trunking:

Supports static port trunking and port trunking with IEEE 802.3ad LACP.

Bandwidth Control:

Supports ingress and egress per port bandwidth control.

Port Security:

Supports allowed, denied forwarding and port security with MAC address.

SNMP/RMON:

SNMP agent and RMON MIB. In the device, the SNMP agent is a client software which is operating over the SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. The SNMP agent will actively issue TRAP information when requested.

RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643), Ethernet MIB (RFC 1643) and so on.

IGMP Snooping:

Supports IGMP version 2 (RFC 2236): IGMP snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

IGMP Proxy:

The implementation of IP multicast processing. The switch supports IGMP version 1 and IGMP version 2, efficient use of network bandwidth, and fast response time for channel changing. IGMP version 1 (IGMPv1) is described in RFC1112, and IGMP version 2 (IGMPv2) is described in RFC 2236. Hosts interact with the system through the exchange of IGMP messages. Similarly, when you configure IGMP proxy, the system interacts with the router on its upstream interface through the exchange of IGMP messages. However, when acting as the proxy, the system performs the host portion of the IGMP task on the upstream interface as follows:

- When queried, sends group membership reports to the group.
- When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership reports to that group.
- When the last of its hosts in a particular multicast group leaves the group, sends an unsolicited leave group membership report to the all-routers group (244.0.0.2).

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

— SG71660MA Layer 2 Managed Switch
— Mounting Accessory (for 19” Rack Shelf)
— This User's Manual on CD-ROM
— AC Power Cord
— RS-232 Cable

Please notify VERSITRON immediately if any of the aforementioned items is missing or damaged.

1-3. Features

The SG71660MA, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

• Hardware

- 12 10/100/1000Mbps Auto-negotiation Ethernet TP ports
- 4 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media ports
- 1392KB on-chip frame buffer
- Supports jumbo frame up to 9600 bytes
- Programmable classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE802.1Q)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE802.1Q Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-16: LINK/ACT, 10/100/1000Mbps, SFP Port 13-16: SFP(LINK/ACT)

• Management

- Supports concisely the status of the ports and provides easy port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system information when you login
- Supports port mirror function
- Supports the static trunk function

- Supports 802.1Q VLAN
- Supports user management and limits three users to login
- Maximum packet length can be up to 9600 bytes for jumbo frame applications
- Supports DHCP Broadcasting Suppression
- Supports to send the trap event while monitored events occur
- Supports default configuration which can be restored to overwrite the current configuration via web browser and CLI
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management and CLI management, providing a more convenient user interface
- Supports port mirror function with ingress/egress traffic
- Supports rapid spanning tree (802.1w RSTP)
- Supports multiple spanning tree (802.1s MSTP)
- Supports 802.1X port security on a VLAN
- Supports IP-MAC-Port Binding for LAN security
- Supports user management where only first login administrator can configure the device. Other users can only view the switch.
- SNMP access can be disabled and prevent unauthorized SNMP access
- Supports Ingress, Non-unicast and Egress Bandwidth rating management with a resolution of 1Mbps
- The trap event and alarm message can be transferred via e-mail
- Supports diagnostics to let administrator know the hardware status
- Supports loop detection to protect the switch from crashing if the networking has a looping issue
- HTTP and TFTP for firmware upgrade, system log upload and configuration file import/export
- Supports remote booting through user interface and SNMP
- Supports NTP network time synchronization and daylight saving
- Supports 120 event log records in the main memory and display on the local console

1-4. Full View of the SG71660MA

Fig. 1-1 Full View of the SG71660MA

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are (12) 10/100/1000 Ethernet ports and (4) SFP fiber ports for optional removable modules on the front panel of the switch. The LED indicators include a Power LED, which indicates the power status of the switch, as well as status indicators for each of the TP ports and SFP ports. One RS-232 DB-9 interface is offered for configuration or management.

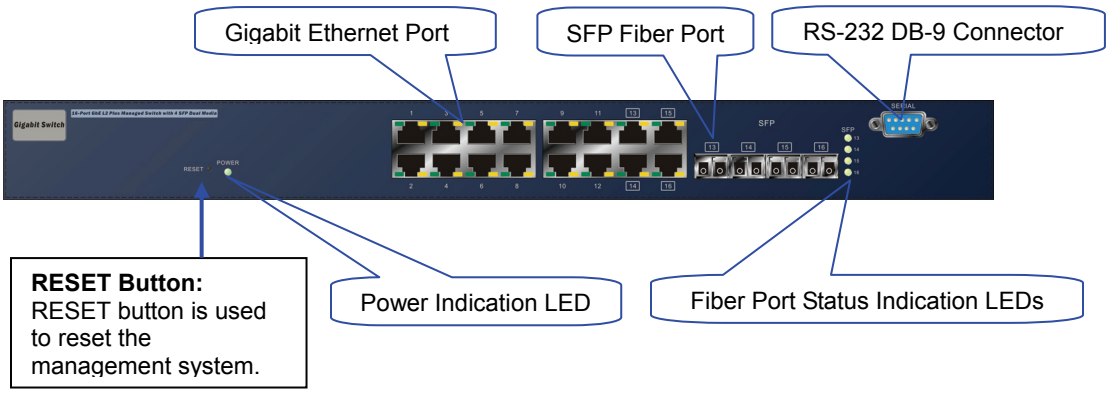

Gigabit Ethernet Port
SFP Fiber Port
RS-232 DB-9 Connector
RESET Button:
RESET button is used to reset the management system.
Power Indication LED
Fiber Port Status Indication LEDs

Fig. 1-2 Front View of the SG71660MA

• LED Indicators

LED	Color	Function
System LED		
POWER	Green	Lit when power is on
10/100/1000Ethernet TP Port 1 to 16 LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present Off when cable connection is not good
10/100/1000Mbps	Green/ Amber	Lit green when 1000Mbps speed is active Lit ember when 100Mbps speed is active Off when 10Mbps speed is active
1000SX/LX Gigabit Fiber Port 13 to 16 LED		
SFP(LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table1-1

1-4-2. AC Power Input on the Rear Panel

One socket on the rear panel is for AC power input.

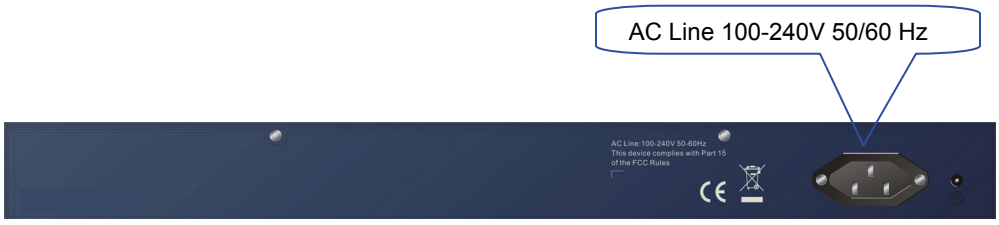


Fig. 1-3 Rear View of SG71660MA

1-5. View of the Optional Modules

Ports 13~16 work with two types of media --- TP and SFP Fiber (LC, BiDi LC…); these ports support 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceivers are used for high-speed connection expansion. The following are optional SFP types available for the switch:

Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

2. Installation

2-1. Starting the SG71660MA

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do the following first:

⇒ Wear a grounding device to avoid damage from electrostatic discharge

• Installing Optional SFP Fiber Transceivers into the SG71660MA

Note: If you do not use SFP modules, please skip this section.

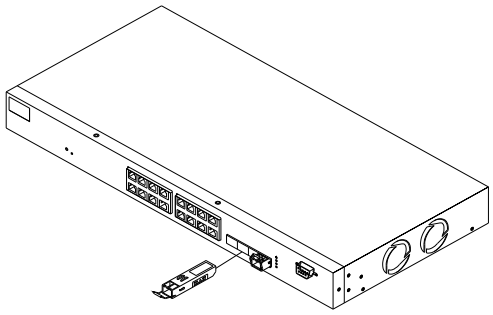


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

• Connecting the SFP Module to the Chassis:

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis.
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector.
3. Install the media cable for network connection.
4. Repeat the above steps, as needed, for each module to be installed.

- **TP Port and Cable Installation**

⇒ On the SG71660MA, the TP ports support MDI/MDI-X auto-crossover, so both types of cables, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.

⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

• Power On

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connections are plugged into the switch or not when powered on, SFP modules as well. After the power is on, all LED indicators will light up immediately and then go off, except for the power LED which remains on. This represents a reset of the system.

• Firmware Loading

After resetting, the boot loader will load the firmware into the memory. This will take about 30 seconds. The witch will flash all the of LEDs once and automatically perform a self-test before going into the ready state.

2-1-2. Installing the SG71660MA into 19-Inch Wiring Closet Rail

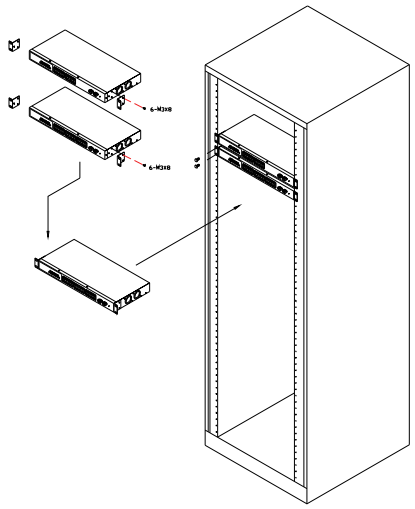


Fig. 2-2

Caution: Allow proper spacing and proper air ventilation for the cooling fan at both sides of the switch.

⇒ Wear a grounding device for electrostatic discharge.
⇒ Screw the mounting accessory to the front side of the switch (See Fig. 2-2).
⇒ Place the switch into the 19-inch wiring closet rail and locate it at the proper position. Then, secure the Chassis with the included screws.

2-1-3. Cabling Requirements

To help ensure a successful installation and keep the network performing well, please use the proper cables. Cables with inadequate specifications will hinder the performance of the network.

2-1-3-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
  — The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.
⇒ Gigabit Ethernet TP network connection
  — The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module

Fiber optic cable is more complex than TP cabling. Basically, there are two categories of fiber, multi-mode (MM) and single-mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there are duplex LC and bidirectional (BIDI) simplex LC.

The SG71660MA supports the following types of fiber optic cables:

— Multi-mode 50/125 micron

— Multi-mode 62.5/125 micron

— Single-mode 9/125 micron

2-1-3-3. Switch Cascading in Topology

• Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading so that you may up-link an unlimited number of switches. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1sec./100 Mega bit)			

Table 2-2

The sum of all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

• Typical Network Topology in Deployment

A hierarchical network with minimum levels of switches may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; and lower the possibility of a network loop, improving network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is a general rule if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-3).

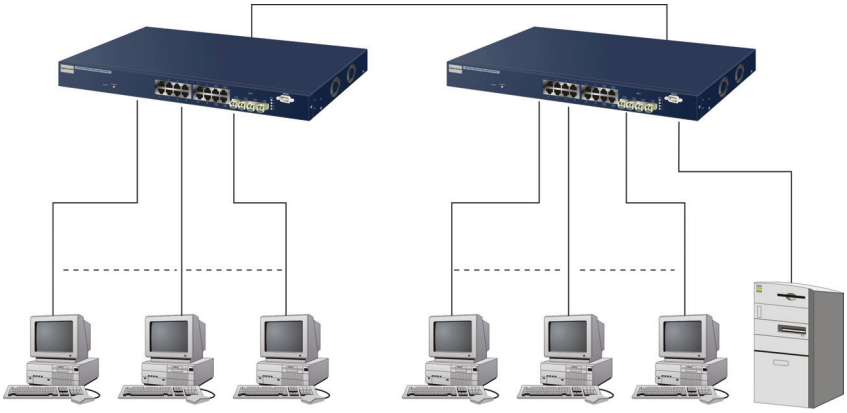


Fig. 2-3 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate with each other directly is bound in the same VLAN area.

Here the VLAN area is defined by which VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the differences are.

Case2a: Port-based VLAN (See Fig.2-4).

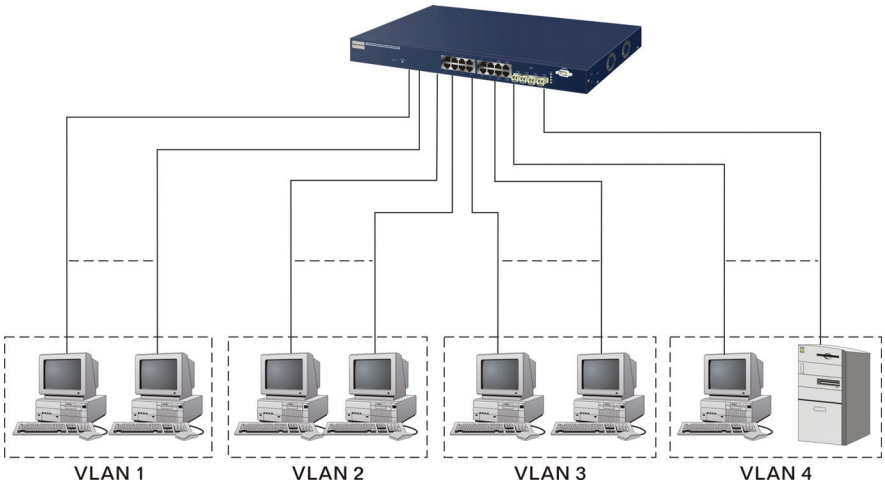


Fig. 2-4 Port-based VLAN Diagram

1. The same VLAN members can not be in different switches.
2. Every VLAN member cannot access every other VLAN member.
3. The switch manager has to assign different names for each VLAN group at one switch.

Case 2b: Port-based VLAN (See Fig.2-5).

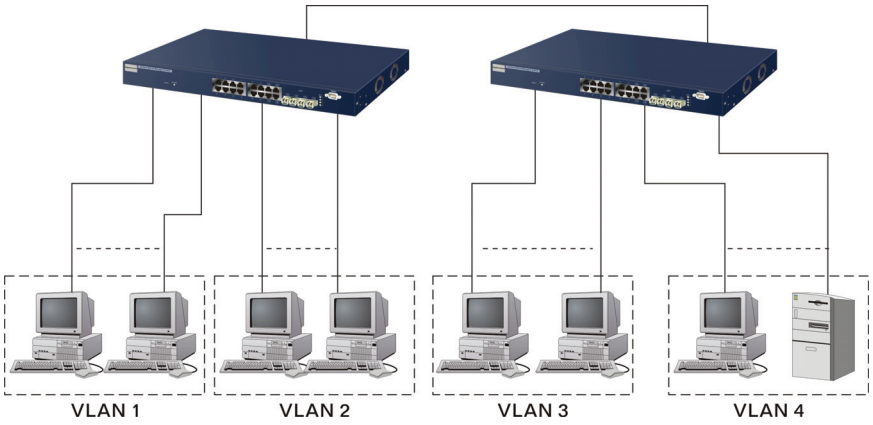


Fig. 2-5 Port-based VLAN Diagram

1. VLAN1 members cannot access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members cannot access VLAN1 and VLAN3 members, but they can access VLAN4 members.
3. VLAN3 members cannot access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members cannot access VLAN1 and VLAN3 members, but they can access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-6).

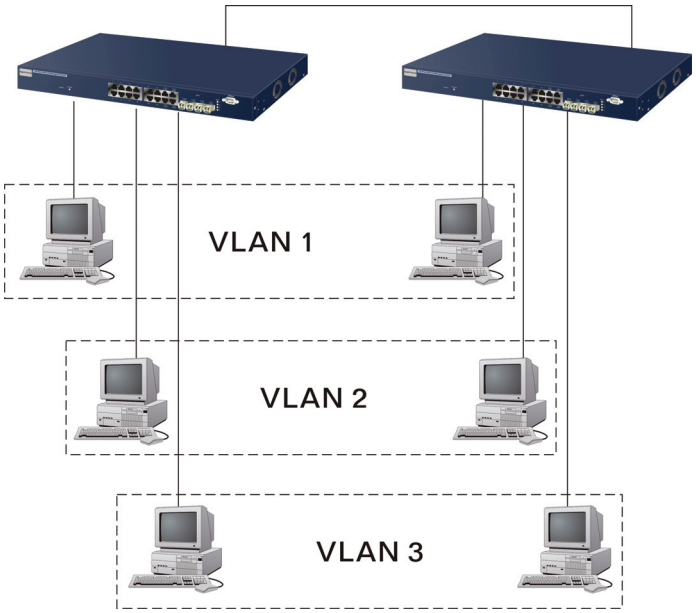


Fig. 2-6 Attribute-based VLAN Diagram

2-1-4. Configuring the Management Agent of the SG71660MA

We offer you three ways to startup the switch management function. They are RS-232 console, CLI, and Web. Users can use any one of them to monitor and configure the switch. You can access them through the following procedures.

Section 2-1-4-1: Configuring the Management Agent of SG71660MA through the Serial RS-232 Port

Section 2-1-4-2: Configuring the Management Agent of SG71660MA through the Ethernet Port

Note: Please first modify the IP address, Subnet mask, Default gateway and DNS through RS-232 console, and then proceed.

2-1-4-1. Configuring the Management Agent of SG71660MA through the Serial RS-232 Port

To perform the configuration through RS-232 console port, the switch's serial port must be directly connected to a DCE device, for example a PC, through an RS-232 cable with a DB-9 connector. Next, run a terminal emulator with the default setting of the switch's serial port. With this, you can communicate with the switch.

In the switch, the RS-232 interface only supports baud rate 115200bps with 8 data bits, 1 stop bit, no parity check and no flow control.

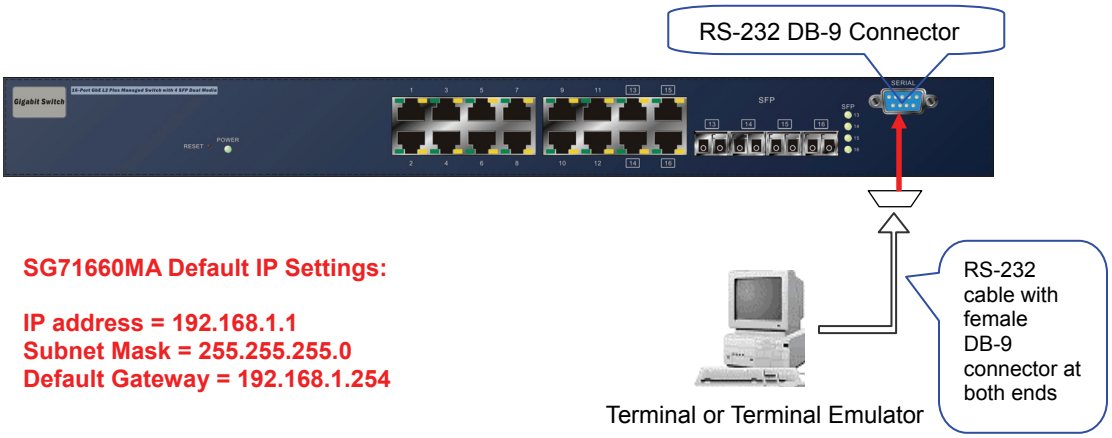

RS-232 DB-9 Connector
SG71660MA Default IP Settings:
IP address = 192.168.1.1
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254
RS-232 cable with female DB-9 connector at both ends
Terminal or Terminal Emulator

Fig. 2-7

To configure the switch, please follow the procedures below:

1. Find the RS-232 DB-9 cable with female DB-9 connector included with the SG71660MA. Normally, it just uses pins 2, 3 and 7. See also Appendix B for more details on Null Modem Cable Specifications.
2. Attach the DB-9 female cable connector to the male serial RS-232 DB-9 connector on the switch.
3. Attach the other end of the serial RS-232 DB-9 cable to PC's serial port, running a terminal emulator supporting VT100/ANSI terminal with The switch's serial port default settings. For example, Windows98/2000/XP HyperTerminal utility.

Note: The switch's serial port default settings are listed as follows:

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4. When you complete the connection, then press **<Enter>** key. The login prompt will be shown on the screen. The default username and password are shown as below:

Username = admin **Password = admin**

• Set IP Address, Subnet Mask and Default Gateway IP Address

Please refer to Fig. 2-7 CLI Management for details about the default factory IP settings. You can first either configure your PC IP address or change IP address of the switch. Next change the default gateway and subnet mask.

For example, your network address is 10.1.1.0, and subnet mask is 255.255.255.0. You can change the switch's default IP address 192.168.1.1 to 10.1.1.1 and set the subnet mask to be 255.255.255.0. Then, choose your default gateway, may be it is 10.1.1.254.

Default Value	SG71660MA	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

Table 2-3

After completing these settings in the switch, it will reboot to have the configuration taken effect. After this step, you can operate the management through the network, using a web browser or Network Management System (NMS).

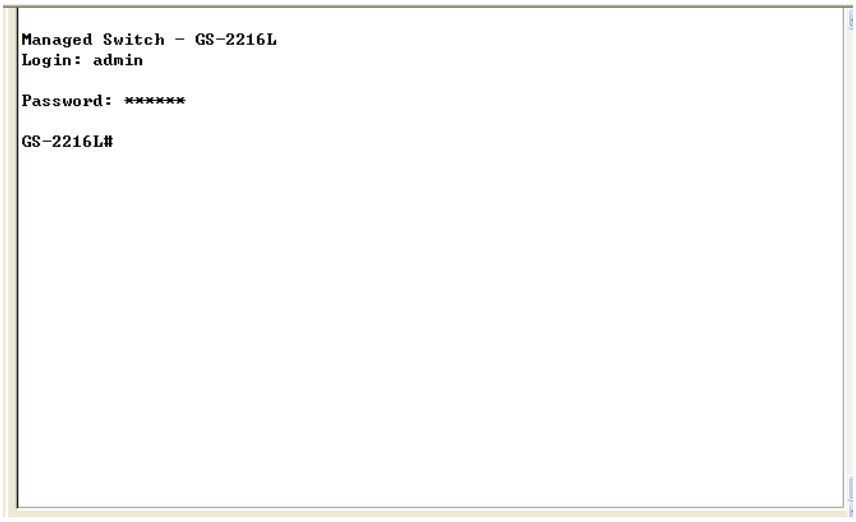


Fig. 2-8 the Login Screen for CLI

NOTE: GS-2216L represents the name of the firmware for the SG71660MA.

2-1-4-2. Configuring the Management Agent of SG71660MA through an Ethernet Port

There are three ways to configure and monitor the switch through the switch's Ethernet port. They are CLI, Web browser and SNMP manager. The user interface for the last one is NMS dependent and is not covered here. We just introduce the first two types of management interface.

SG71660MA Default IP Settings:

IP address= 192.168.1.1
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254

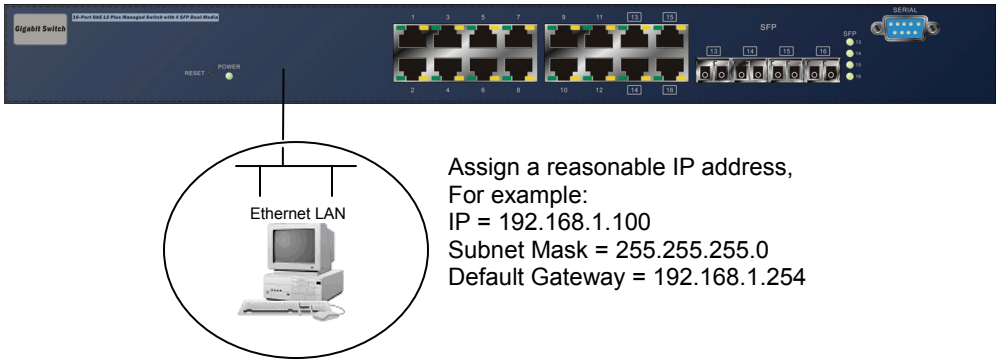


Fig. 2-9

• Managing SG71660MA through Ethernet Port

Before you communicate with the switch, you first have to finish the configuration of the IP address or know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC using UTP Cat. 5 cable with RJ-45 connector.

   Note: If the PC is connected directly to the switch, you have to setup the same subnet mask between them. But, the subnet mask may be different for the PC in a remote site. Please refer to Fig. 2-9 about the switch's default IP address information.

2. Run CLI or web browser and follow the menu. Please refer to Chapter 3 and Chapter 4.

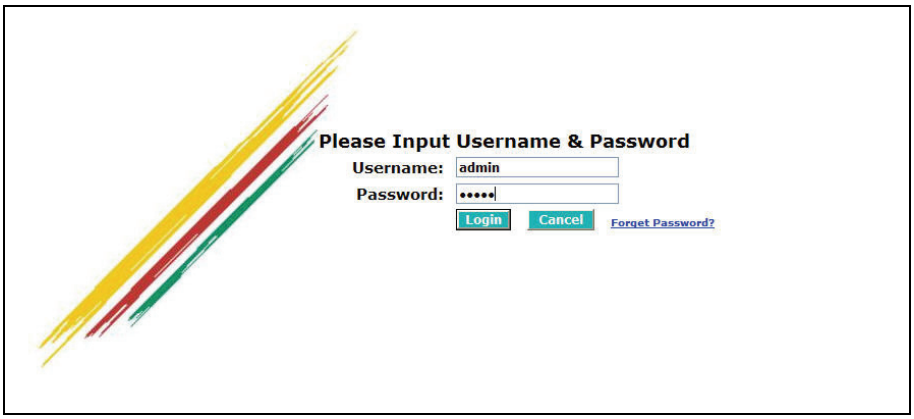


Fig. 2-10 the Login Screen for Web

2-1-5. IP Address Assignment

For IP address configuration, there are three parameters that are required. They are the IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks as shown in the Fig. 2-11. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

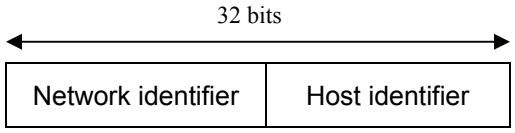
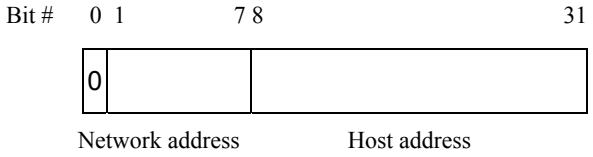


Fig. 2-11 IP address structure

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

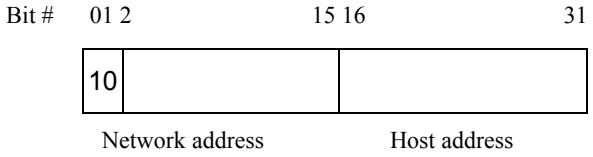
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks that can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



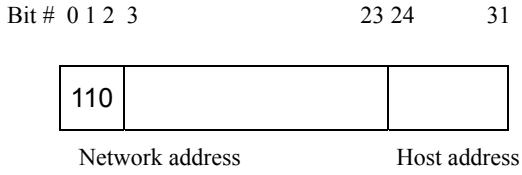
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP addresses range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal networks. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

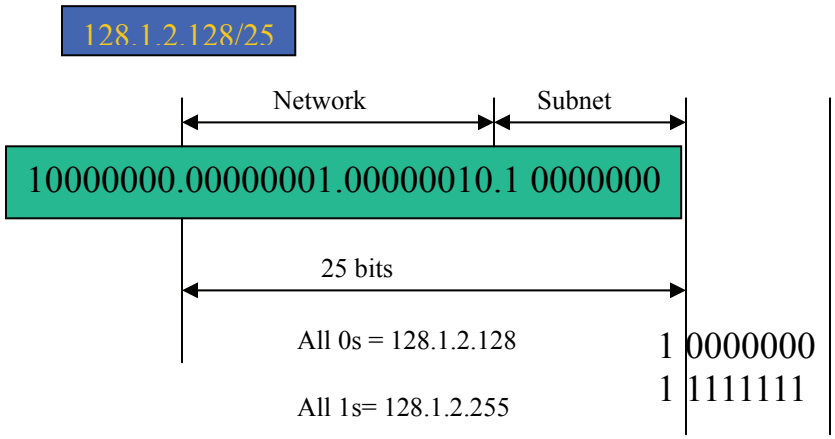
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP addresses more efficiently and make it easier to manage an IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 by default, in which the first two bytes are with all 1s. This means more than 60 thousand nodes in flat IP addresses will be at the same network. It's too large to manage practically. Now if we divide it into smaller networks by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes are used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP addresses are available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what would a reserved IP address look like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-4

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will be a maximum of 254 effective nodes existent in this sub-netted network and it is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy. The gateway setting is only used for Trap Events Host in the switch.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

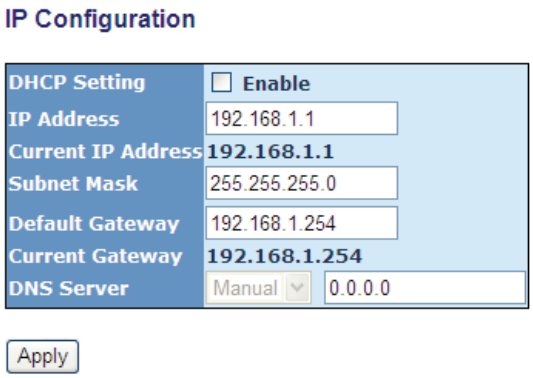


Fig. 2-12

First, IP Address: as shown in the Fig. 2-12, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-12, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

The Domain Name Server translates human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, the user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

2-2. Typical Applications

The SG71660MA implements 12 Gigabit Ethernet TP ports with auto MDIX and 4 slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central Site/Remote site application used in carrier or ISP (See Fig. 2-13)
- Peer-to-peer application used in two remote offices (See Fig. 2-14)
- Office network(See Fig. 2-15)

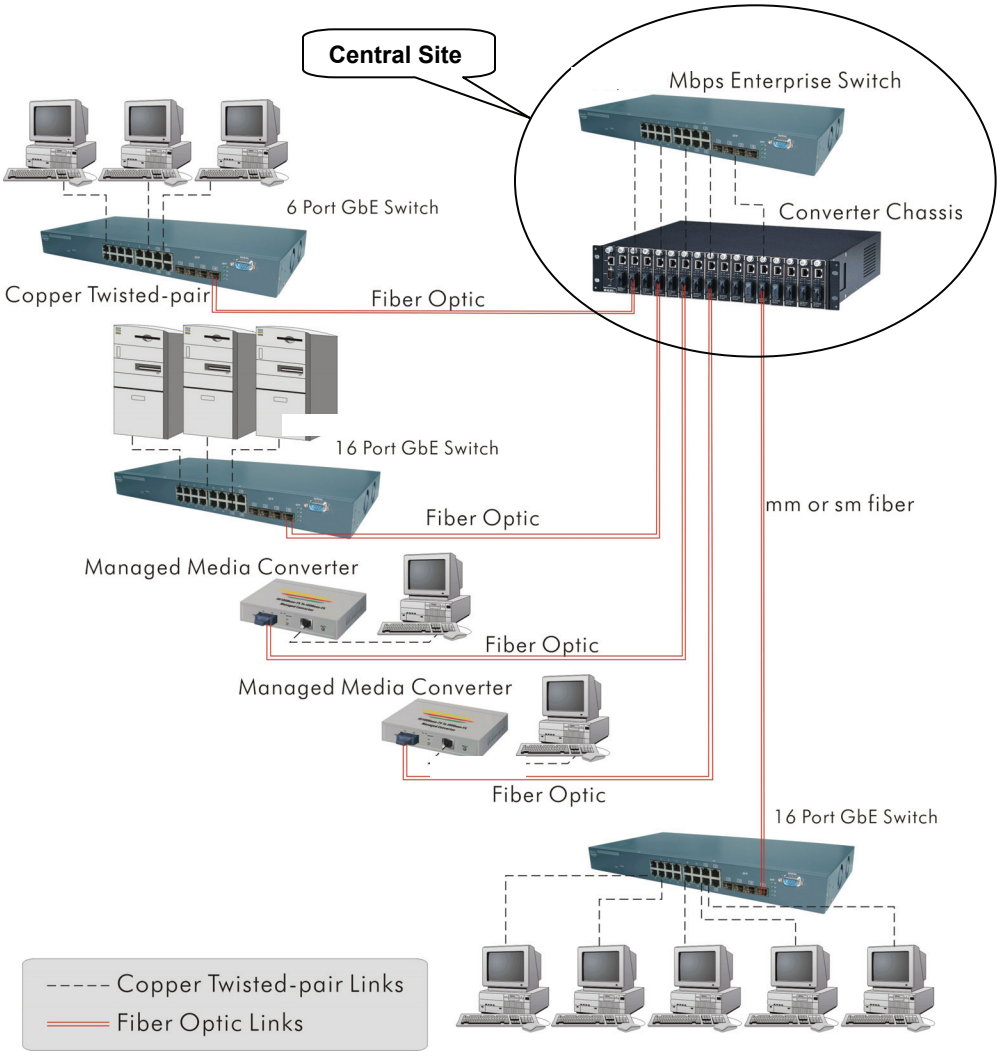


Fig. 2-13 Network Connection between Remote Site and Central Site

Fig. 2-13 is a system-wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

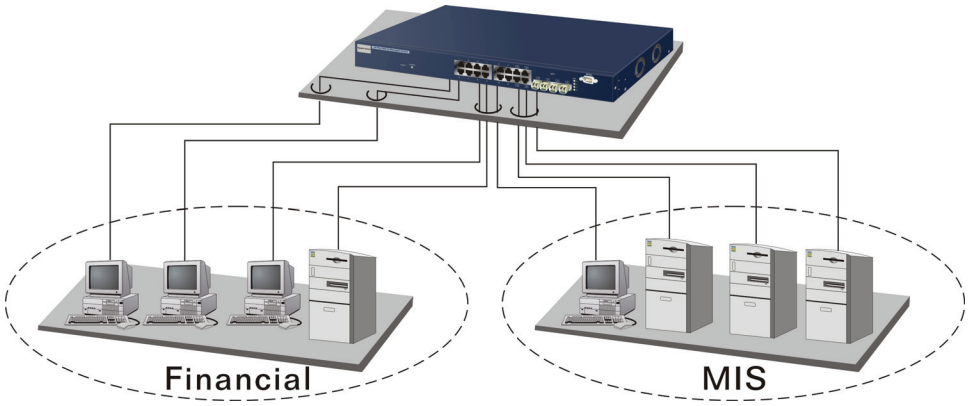


Fig. 2-14 Peer-to-peer Network Connection

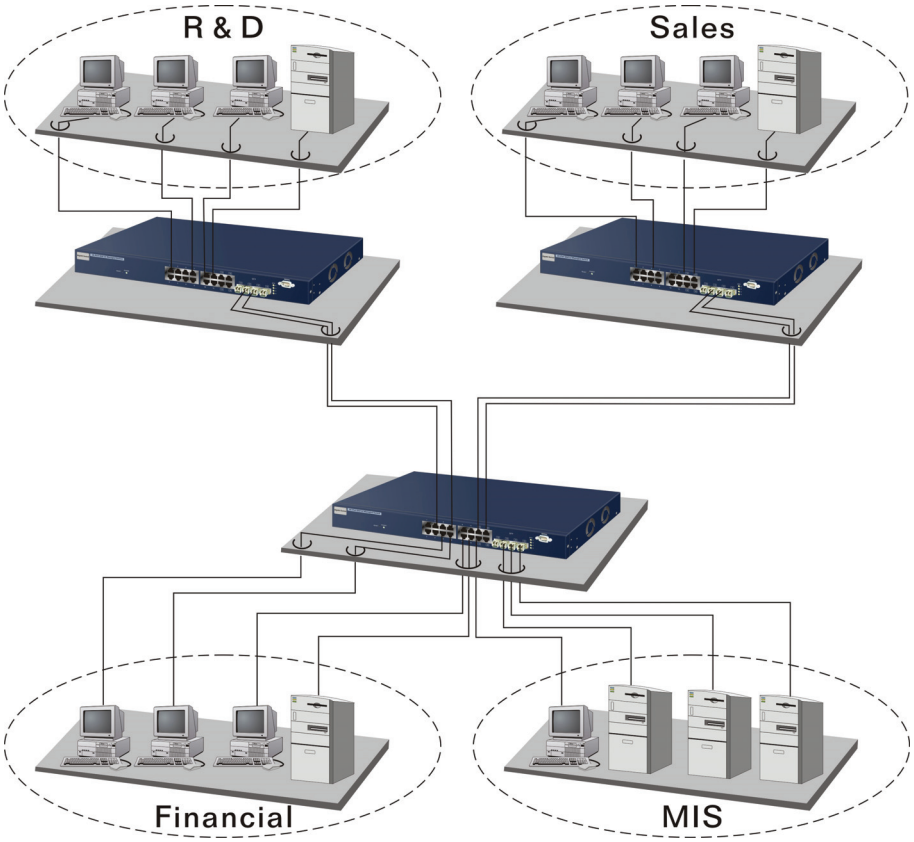


Fig. 2-15 Office Network Connection

3. Operation of Web-based Management

This chapter instructs you how to configure and manage the SG71660MA through the web user interface. With this facility, you can easily access and monitor the status of the switch, including MIBs status, each port's activity, Spanning Tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access records and so on.

The default values of the managed switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

Table 3-1

After the switch has been configured using the CLI via the switch's serial interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.3-1) and ask you to input the username and password in order to login and access authentication. The default username and password are both "admin". Please enter the default username and password, then click the **<Login>** button. The login process now is completed.

Just click the link of "Forget Password" in WebUI (See Fig. 3-1) or input "Ctrl+Z" in CLI's login screen (See Fig. 4-1~4-2) in case the user forgets the manager's password. Then, the system will display a serial No. for the user. Write down this serial No. and contact VERSITRON who will supply you with a temporary password. Use this new password as ID and Password, and it will allow the user to log into the system temporarily. Due to the limit of this new password, the user only can login the system one time. Therefore, please modify your password immediately after you login successfully.

In this login menu, you have to input the complete username and password respectively. The switch will not give you a shortcut to username automatically. This may seem inconvenient, but it is safer.

In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch.

To optimize the display, we recommend you use Microsoft IE 6.0 or above, Netscape v7.1 or above, or Firefox v1.00 or above and set the resolution to 1024x768.

In Fig. 3-2, for example, the left section is the whole function tree within the web user interface and we will show this throughout this chapter.

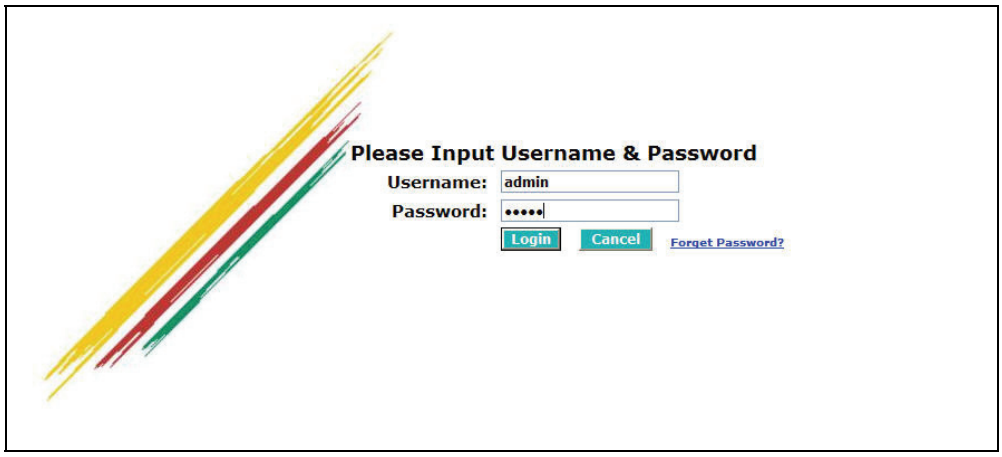


Fig. 3-1

3-1. Web Management Home Overview

After you login, the switch shows you the system information as shown in Fig. 3-2. This page is the default and tells you the basic information of the system, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size” and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports are used and so on.

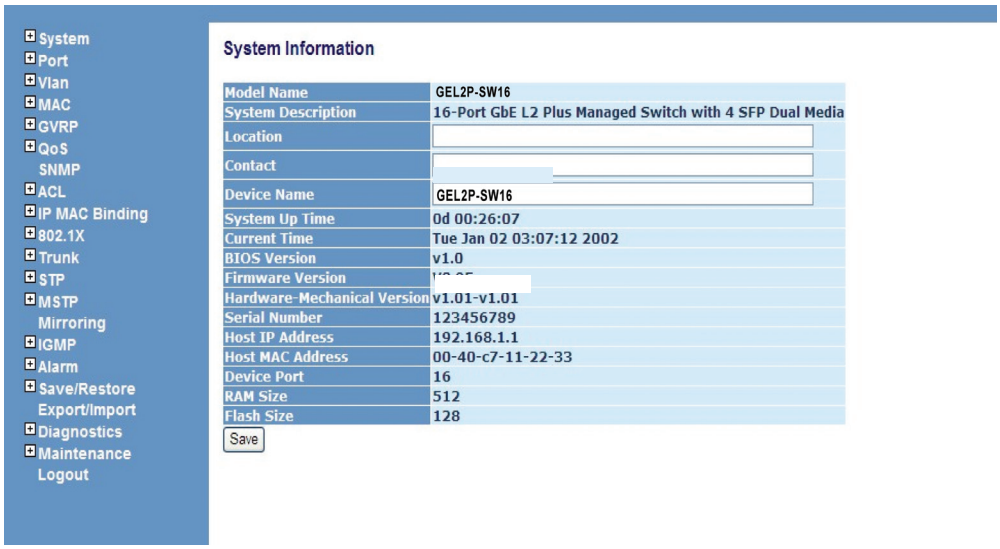


Fig. 3-2

• The Information of Page Layout

— On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; the unlinked ports will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of the module depends on the one you inserted. The same, if disconnected, the port will be dark, if linked, green. (See Fig. 3-3)

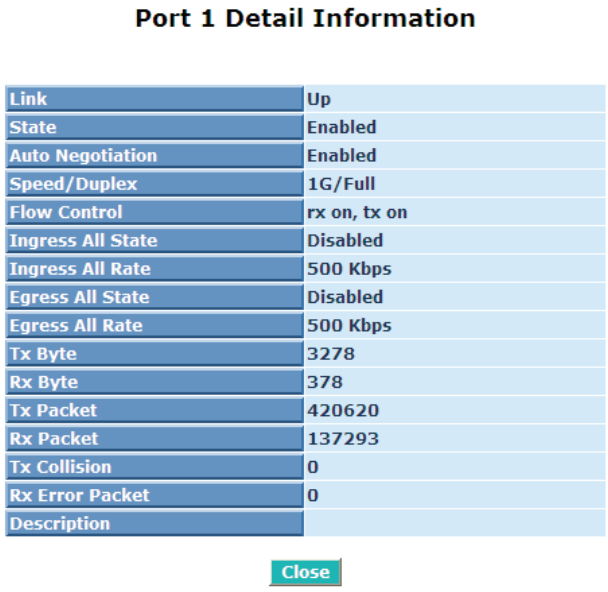
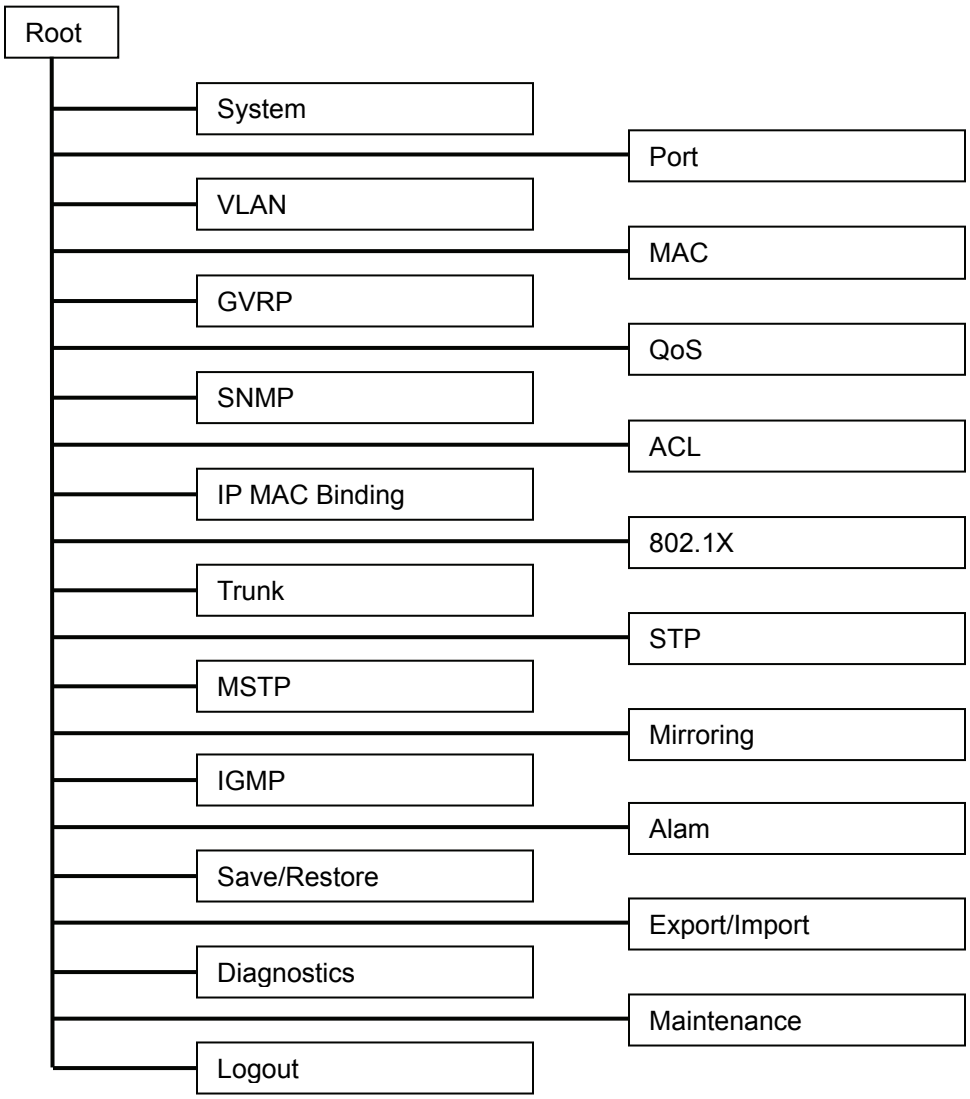


Fig. 3-3 port detail information

In Fig. 3-3, it shows the basic information of the clicked port. With this, you'll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.

— In the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action ids detected on the device for 3 minutes. If OFF is chosen, the screen will stay as it is. Default is ON.

— On the left side, the main menu tree is listed on the page. The menu is hierarchical. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponding section respectively. When clicking it, the function is performed. The following list is the full function tree for web user interface.


Root
System
Port
VLAN
MAC
GVRP
QoS
SNMP
ACL
IP MAC Binding
802.1X
Trunk
STP
MSTP
Mirroring
IGMP
Alam
Save/Restore
Export/Import
Diagnostics
Maintenance
Logout

3-1-1. System Information

Function name:

System Information

Function description:

Show the basic system information.

Parameter description:

Model name:

The model name of this device.

System description:

This tells what this device is. For example, “SG71660MA Managed Switch”.

Location:

Basically, it is the location where this switch is installed. User-defined.

Contact:

For easily managing and maintaining the device, you may write down the contact person and phone number here. You can configure this parameter through the device’s user interface or SNMP.

Device name:

The name of the switch. User-defined. Default is 16 GIGABIT L2 PLUS MANAGED SWITCH.

System up time:

The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Current time:

Shows the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.

BIOS version:

The version of the BIOS in this switch.

Firmware version:

The firmware version in this switch.

Hardware-Mechanical version:

The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.

Serial number:

The serial number assigned during manufacturing.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Shows all types and numbers of the ports in the switch.

RAM size:

The size of the DRAM in this switch.

Flash size:

The size of the flash memory in this switch.

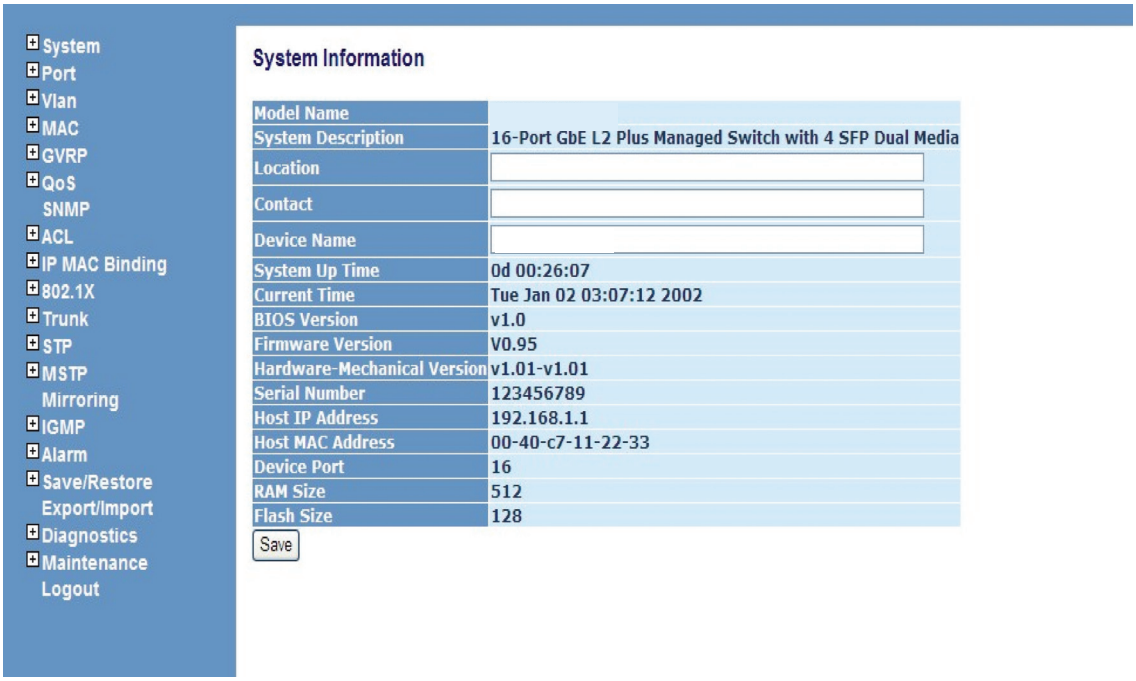


Fig. 3-4

3-1-2. Account Configuration

In this function, only the administrator can create, modify or delete the username and password. The administrator can modify other guest identities' passwords without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identities can modify his or her password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and cannot be deleted. In addition, up to 4 guest accounts can be created.

The default setting for user account is:

Username : admin

Password : admin

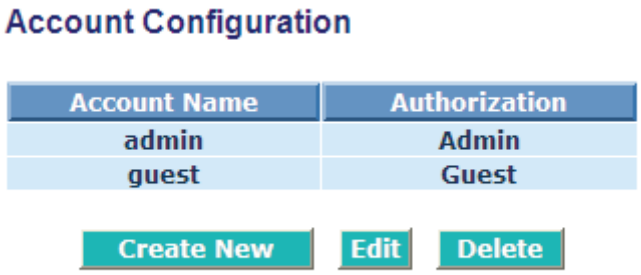


Fig. 3-5

3-1-3. Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses residing in the Internet and a user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area’s time adjustment.

Parameter description:

Current Time:

Show the current time of the system.

Manual:

This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press **<Apply>** button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press **<Apply>** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1
Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to sync the network time based on Greenwich Mean Time (GMT). If using the NTP mode and selecting a built-in NTP time server or manually specifying a user-defined NTP server as well as Time Zone, the switch will sync the time shortly after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without the user processing this action.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to arrive at the local time, Otherwise, you will not be able to get the correct time. The switch supports configurable time zone from –12 to +13 in 1 hour increments.

Default Time zone: +8 Hrs.

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time of –5 ~ +5 in 1 hour increments. The zero for this parameter means it does not need to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start :

This is used to set when to start performing the day light saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Day Light Saving End :

This is used to set when to stop performing the daylight saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

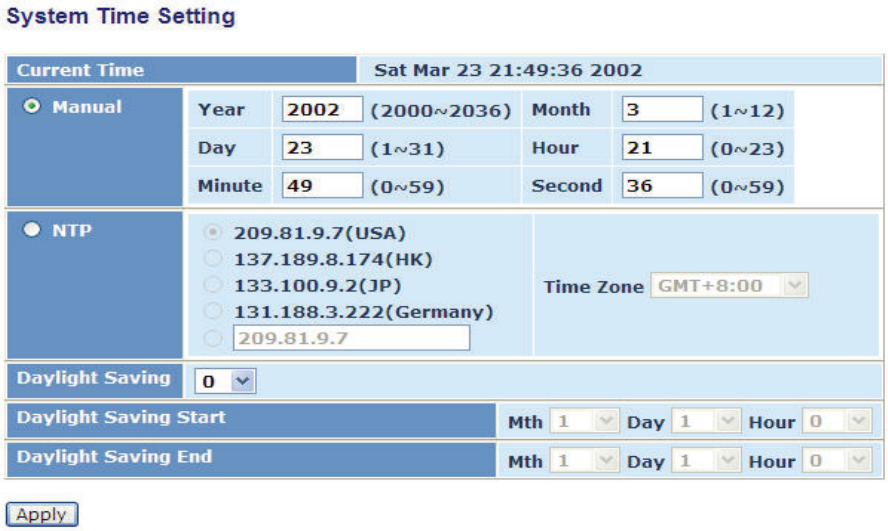

System Time Setting
Current Time
Sat Mar 23 21:49:36 2002
Manual
Year
2002
(2000~2036)
Month
3
(1~12)
Day
23
(1~31)
Hour
21
(0~23)
Minute
49
(0~59)
Second
36
(0~59)
NTP
209.81.9.7(USA)
137.189.8.174(HK)
133.100.9.2(JP)
131.188.3.222(Germany)
209.81.9.7
Time Zone
GMT+8:00
Daylight Saving
0
Daylight Saving Start
Mth
1
Day
1
Hour
0
Daylight Saving End
Mth
1
Day
1
Hour
0
Apply

Fig. 3-6

3-1-4. IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, the network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting take affect and use the new IP to browse for web management and CLI management.

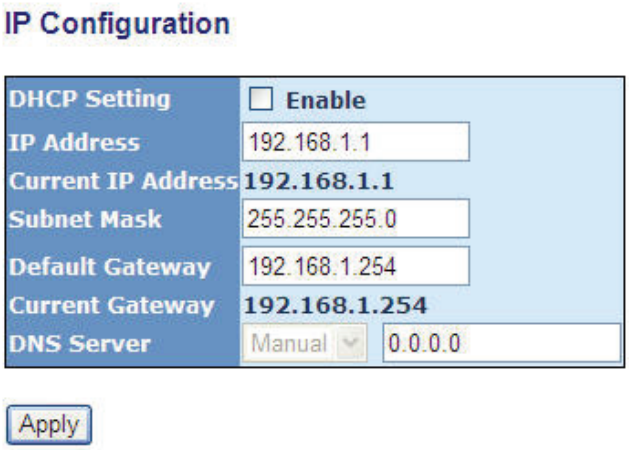


Fig. 3-7 IP Address Configuration

Function name:

IP Configuration

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

The switch supports DHCP client to get an IP address automatically if you set this function to “Enable”. When enabled, the switch will issue the request to the DHCP server residing on the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If this field is set to “Disable”, you’ll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 “IP Address Assignment” in this manual.

Default: Disable

IP address:

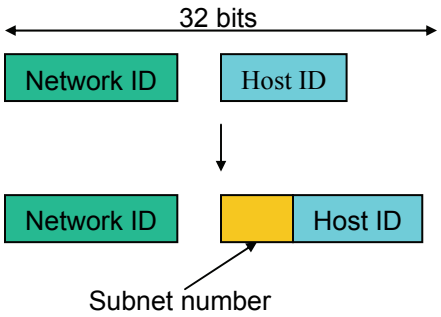
Users can configure the IP settings and fill in new values if users set the DHCP function “Disable”. Then, click **<Apply>** button to update.

When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is filled by DHCP server and will not allow the user to manually set it.

Subnet mask:

Subnet mask is made for the purpose of getting more network addresses because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise it can’t communicate with other devices. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from the host address and makes an IP address comprised of Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total number of IP addresses a network can support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices residing on the same network.

For more information, please also see the Section 2-1-5 “IP Address Assignment” in this manual.

Default: 255.255.255.0

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS:

Domain Name Server is used to serve the translation between IP address and name address.

The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

Default: 0.0.0.0

3-1-5. Loop Detection

Loop detection is used to detect the presence of traffic. When the switch receives a packet's (looping detection frame) MAC address the same port as it was sent, show Loop detection happens. The port will be locked when it receives the looping detection frames. If you want to resume using the locked port, please find the looped path and correct. Then select the locked port and click on "Resume" to turn on the locked ports.

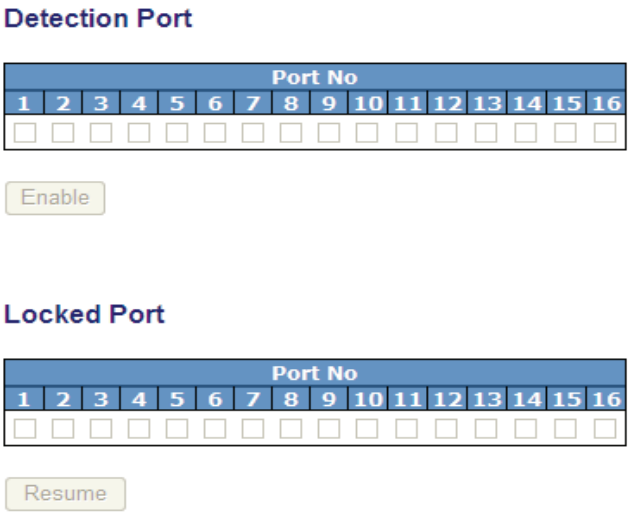


Fig. 3-8

Function name:

Loop Detection

Function description:

Display whether switch open Loop detection.

Parameter description:

Port No:

Display the port number. The number is 1 – 16.

Detection Port - Enable:

When a Port No is chosen and Loop Detection is enabled, the port can detect loops. If a loop is detected the port will be Locked. If a loop is not detected, the port maintains Unlocked.

Locked Port - Resume:

When a loop is detected and the port is locked, the user can correct the loop and the resume use of the port.

3-1-6. Management Policy

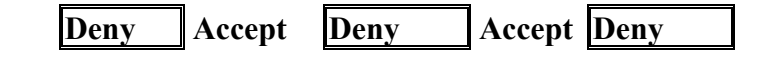
Through the management security configuration, the manager can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the manager to manage the switch:

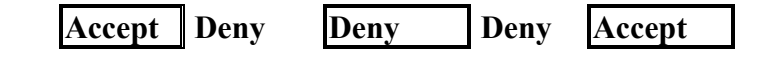
Rule 1) : When no lists exists, then it will accept all connections.

Rule 2) : When only "accept lists" exist, then it will deny all connections, excluding the connection inside of the accepting range.

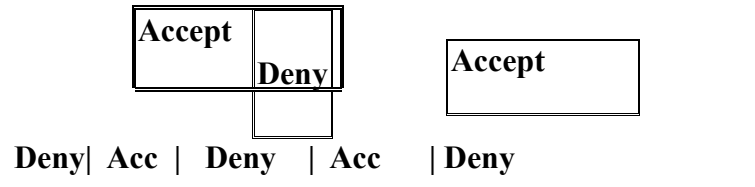
Rule 3) : When only "deny lists" exist, then it will accept all connections, excluding the connection inside of the denying range.



Rule 4) : When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range.



Rule 5) : When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.



Function name:

Management Security Configuration

Function description:

The switch offers a Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user uses to connect to the switch. For example, we can decide which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is connected to could be allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.

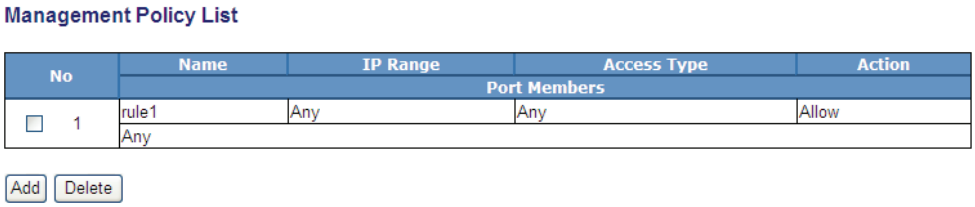


Fig. 3-9

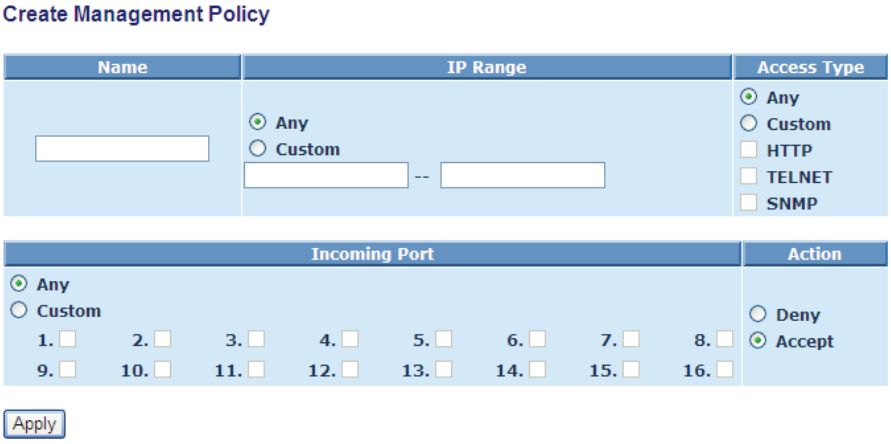


Fig. 3-10

Parameter description:

Add:

A new entry of Management Security Configuration can be created after the parameters as mentioned above have been setup and then press **<Add>** button. Of course, the existing entry also can be modified by pressing this button.

Delete:

Remove the existing entry of Management Security Configuration from the management security table.

Name:

A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximum 8 characters.

VID:

The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom”. Default is “Any”. When you choose “Custom”, you can fill in VID number. The valid VID range is 1~4094.

IP Range:

The switch supports two kinds of options for managing valid IP Range, including “Any” and “Custom”. Default is “Any”. If “Custom” has been chosen, you can assign an effective IP range. The valid range is 0.0.0.0~255.255.255.255.

Incoming Port:

The switch supports two kinds of options for managing valid Port Range, including “Any” and “Custom”. Default is “Any”. You can select the ports that you would like to work or restrict in the management security configuration if “Custom” has been chosen.

Access Type:

The switch supports two kinds of options for managing valid Access Type, including “Any” and “Custom”. Default is “Any”. “Http”, “Telnet” and “SNMP” are three ways for accessing and managing the switch in if “Custom” has been chosen.

Action:

The switch supports two kinds of options for managing valid Action Type, including “Deny” and “Accept”. Default is “Deny”. When you choose “Deny”, you will be restricted and refused to manage the switch due to the “Access Type” you choose. However, when you select “Accept”, you will have the authority to manage the switch.

3-1-7. System Log

The System Log provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

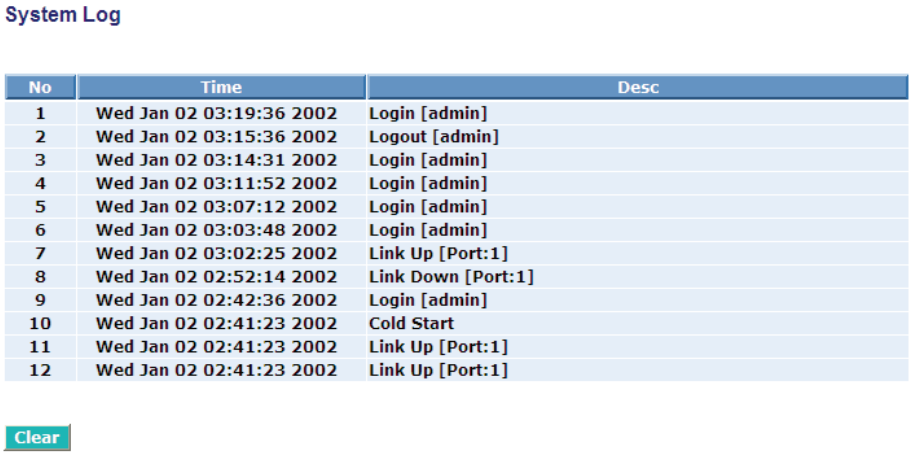

System Log
No
Time
Desc
1 Wed Jan 02 03:19:36 2002 Login [admin]
2 Wed Jan 02 03:15:36 2002 Logout [admin]
3 Wed Jan 02 03:14:31 2002 Login [admin]
4 Wed Jan 02 03:11:52 2002 Login [admin]
5 Wed Jan 02 03:07:12 2002 Login [admin]
6 Wed Jan 02 03:03:48 2002 Login [admin]
7 Wed Jan 02 03:02:25 2002 Link Up [Port:1]
8 Wed Jan 02 02:52:14 2002 Link Down [Port:1]
9 Wed Jan 02 02:42:36 2002 Login [admin]
10 Wed Jan 02 02:41:23 2002 Cold Start
11 Wed Jan 02 02:41:23 2002 Link Up [Port:1]
12 Wed Jan 02 02:41:23 2002 Link Up [Port:1]
Clear

Fig. 3-11

Function name:

System Log

Function description:

The Trap Log Data displays log items including all SNMP Private Trap events, SNMP Public traps and user logs which have occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

Parameter description:

No:

Display the order number that the trap happened.

Time:

Display the time that the trap happened.

Desc:

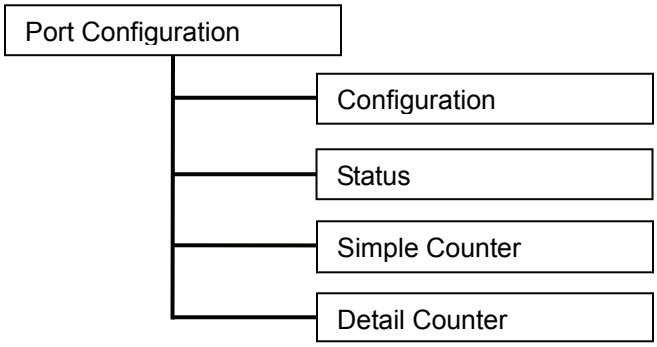
Displays a description event recorded in the System Log.

Clear:

Clear log data.

3-2. Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail in the following sections.



3-2-1. Port Configuration

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.

Port Configuration

Port	Speed	Flow Control	Maximum Frame	Excessive Collision Mode	Description
1	Auto	☑	9600	Discard	
2	Auto	☑	9600	Discard	
3	Auto	☑	9600	Discard	
4	Auto	☑	9600	Discard	
5	Auto	☑	9600	Discard	
6	Auto	☑	9600	Discard	
7	Auto	☑	9600	Discard	
8	Auto	☑	9600	Discard	
9	Auto	☑	9600	Discard	
10	Auto	☑	9600	Discard	
11	Auto	☑	9600	Discard	
12	Auto	☑	9600	Discard	
13	Auto	☑	9600	Discard	
14	Auto	☑	9600	Discard	
15	Auto	☑	9600	Discard	
16	Auto	☑	9600	Discard	

Fig. 3-12

Function name:

Port Configuration

Function description:

It is used to set each port's operation mode. The switch supports 3 parameters for each port. They are state, mode and flow control.

Parameter description:

Speed:

Set the speed and duplex of the port. In speed, if the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

There are two modes to choose in flow control, including Enable and Disable. If flow control is set to Enable, both parties can send PAUSE frames to the transmitting device(s) if the receiving port is too busy. When it is set to Disable, there will be no flow control in the port. The port drops the packet if it is too busy.

Maximum Frame:

1518~9600 (Bytes)

Excessive Collision Mode:

There are two modes to choose when excessive collisions happen in half-duplex condition as below:

Discard: The "Discard" mode determines whether the MAC drops frames after an excessive collision has occurred. If set, a frame is dropped after excessive collisions. This is IEEE Std 802.3 half-duplex flow control operation.

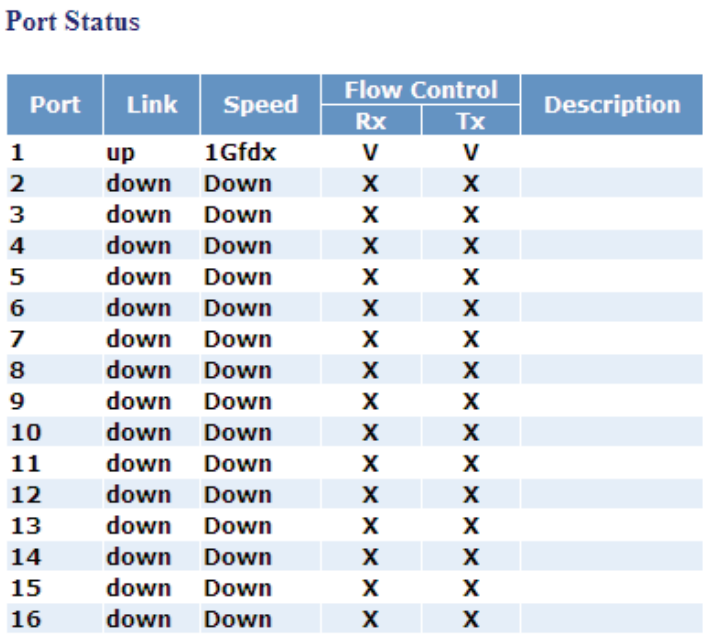
Restart: The "Restart" mode determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Std 802.3, but is useful in non-dropping half-duplex flow control operation.

Description:

Description of device ports can not include " # % & ' + \.

3-2-2.Port Status

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. An extra media type information for the module ports 12 and 16 is also offered (See Fig. 3-14).



Port Status

Port	Link	Speed	Flow Control		Description
			Rx	Tx	
1	up	1Gfdx	V	V	
2	down	Down	X	X	
3	down	Down	X	X	
4	down	Down	X	X	
5	down	Down	X	X	
6	down	Down	X	X	
7	down	Down	X	X	
8	down	Down	X	X	
9	down	Down	X	X	
10	down	Down	X	X	
11	down	Down	X	X	
12	down	Down	X	X	
13	down	Down	X	X	
14	down	Down	X	X	
15	down	Down	X	X	
16	down	Down	X	X	

Fig. 3-13

Function name:

Port Status

Function Description:

Reports the latest updated status of all ports in this switch. When any one of the ports in the switch changes a parameter displayed on the page, it will be automatically refreshed approximately every 5 seconds.

Parameter Description:

Port:

Displays the port number. The number is 1 – 16. Ports 13 ~ 16 can use optional modules.

Link:

Shows if the link on the port is active or not. If the link is connected to an active device, the link will be "Up". Otherwise, it will show "Down". This is determined by the hardware on both ends of the connection.

No default value.

Speed / Duplex Mode:

Displays the speed and duplex of all ports. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in "Auto Speed" mode or 2) user setting in "Force" mode.

Default: None, depends on the result of the negotiation.

Flow Control:

Show each port's flow control status.

There are two types of flow control in Ethernet, Backpressure for half-duplex operation and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of them.

Default: None, depends on the result of the negotiation.

Description:

network managers provide a description of device ports.

Parameter description of Port 13 ~ Port 16:

Note: If you want to see the detailed information shown below, right click on the SFP icon.

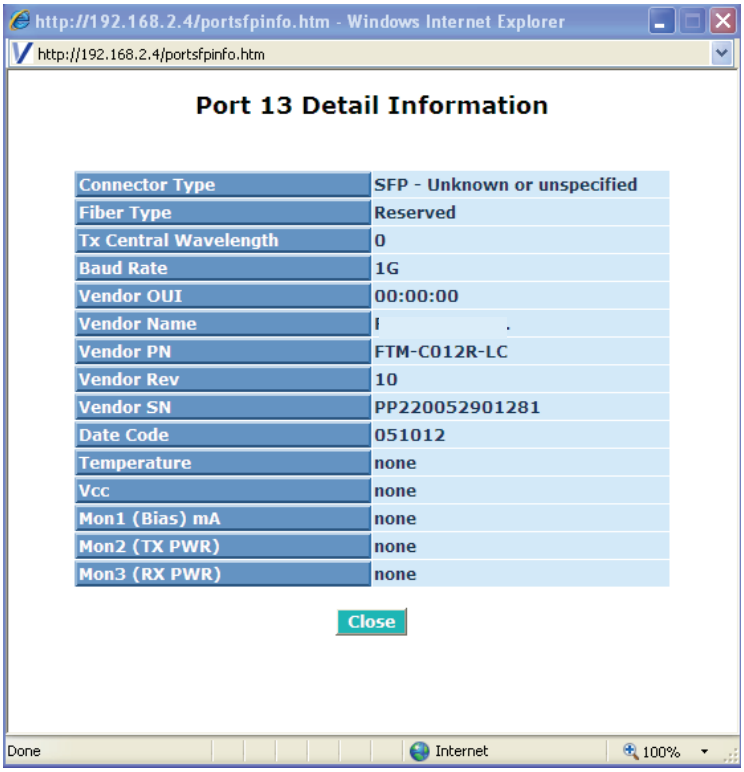


Fig. 3-14

Connector Type:

Displays the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type:

Displays the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength:

Displays the fiber optic transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.

Vendor OUI:

Displays the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name:

Displays the company name of the module manufacturer.

Vendor P/N:

Displays the product name provided by the module manufacturer.

Vendor Rev (Revision):

Displays the module revision.

Vendor SN (Serial Number):

Displays the serial number assigned by the manufacturer.

Date Code:

Displays the date this SFP module was made.

Temperature:

Displays the current temperature of SFP module.

Vcc:

Displays the working DC voltage of SFP module.

Mon1(Bias) mA:

Displays the Bias current of SFP module.

Mon2(TX PWR):

Displays the transmit power of SFP module.

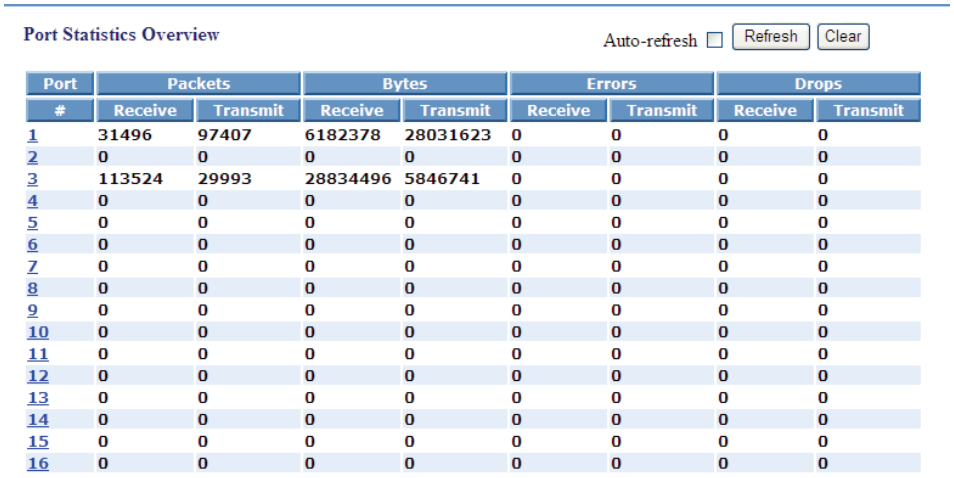
Mon3(RX PWR):

Displays the receiver power of SFP module.

3-2-3. Simple Counter

The function of Simple Counter collects any information and provides the counting of the traffic of the port, regardless if the packet is good or bad.

In the Fig. 3-15, the window can show all ports' counter information at the same time. Each data field is 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The Refresh Interval is used to set the update frequency.



Port	Packets		Bytes		Errors		Drops	
#	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	31496	97407	6182378	28031623	0	0	0	0
2	0	0	0	0	0	0	0	0
3	113524	29993	28834496	5846741	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0

Fig. 3-15

Function name:

Simple Counter

Function description:

Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

Parameters description:

Packet:

Transmit::

The counting number of the packets transmitted.

Receive:

The counting number of the packets received.

Bytes:

Transmit::

Total transmitted bytes.

Receive:

Total received bytes.

Error:

Transmit::

Number of bad packets transmitted.

Receive:

Number of bad packets received.

Drops

Transmit::

Number of transmitted packets dropped.

Receive:

Number of received packets dropped.

Auto-refresh:

The simple counts will be refreshed automatically on the UI screen.

Refresh:

The simple counts will be refreshed manually when user clicks on the “Refresh” button.

Clear:

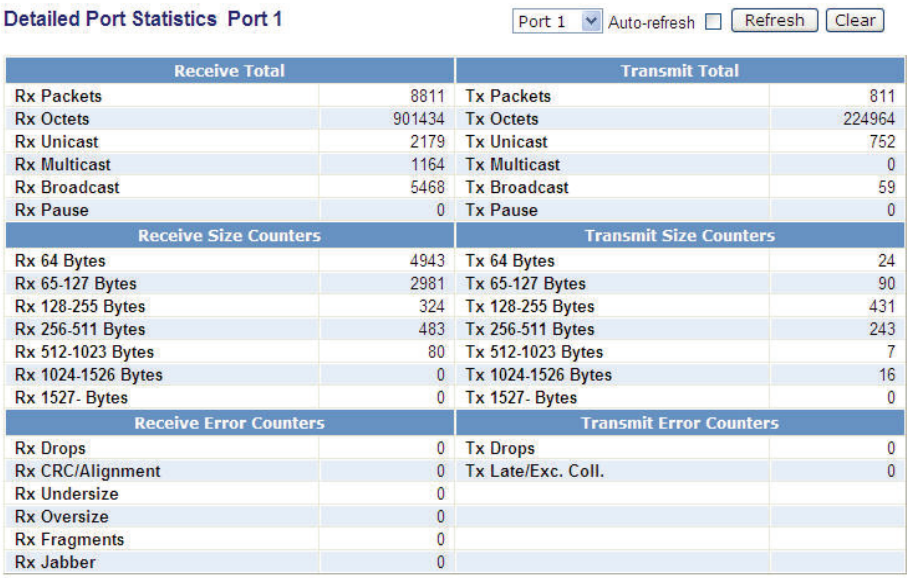
The simple counts will be reset to zero when user clicks on the “Clear” button.

3-2-4. Detail Counter

The function of Detail Counter collects any information and provides the counting of the traffic of the port, regardless if the packet is good or bad.

In the Fig. 3-16, the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

Each data field is 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.



Receive Total		Transmit Total	
Rx Packets	8811	Tx Packets	811
Rx Octets	901434	Tx Octets	224964
Rx Unicast	2179	Tx Unicast	752
Rx Multicast	1164	Tx Multicast	0
Rx Broadcast	5468	Tx Broadcast	59
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	4943	Tx 64 Bytes	24
Rx 65-127 Bytes	2981	Tx 65-127 Bytes	90
Rx 128-255 Bytes	324	Tx 128-255 Bytes	431
Rx 256-511 Bytes	483	Tx 256-511 Bytes	243
Rx 512-1023 Bytes	80	Tx 512-1023 Bytes	7
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	16
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		

Fig. 3-16

Function name:

Detail Counter

Function description:

Display the detailed counting number of each port's traffic. In the Fig. 3-14, the window can show all counter information of each port at one time.

Parameter description:

Rx Packets:

The counting number of the packets received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Shows the counting number of the received broadcast packets.

Rx Multicast:

Shows the counting number of the received multicast packets.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packets.

Tx Multicast:

Shows the counting number of the transmitted multicast packets.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according tomax_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Rx Errors:

Number of the error packets received.

Tx Collisions:

Number of collision transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops:

Number of frames dropped due to the lack of transmitting buffer.

Auto-refresh:

The detail counts will be refreshed automatically on the UI screen.

Refresh:

The detail counts will be refreshed manually when user clicks on the “Refresh” button.

Clear:

The detail counts will be reset to zero when user clicks on the “Clear” button.

3-3. VLAN

The switch supports Tag-based VLAN (802.1Q) and Port-based VLAN. Supports 4094 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into smaller LANs as required. Properly configuring it, you can gain not only improved security and increased performance but greatly reduced VLAN management.

3-3-1. VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag- based, Metro Mode, Double-tag and Disable, you can choose one of them by pulling down list and selecting an item. Then, click **<Apply>** button, the settings will take effect immediately.

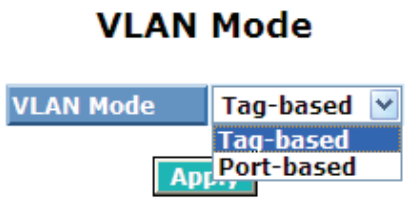


Fig. 3-17

Parameter description:

VLAN Mode:

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximum 16 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 4094 Tag VLAN groups.

3-3-2. Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

It shows the information of existing Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID.

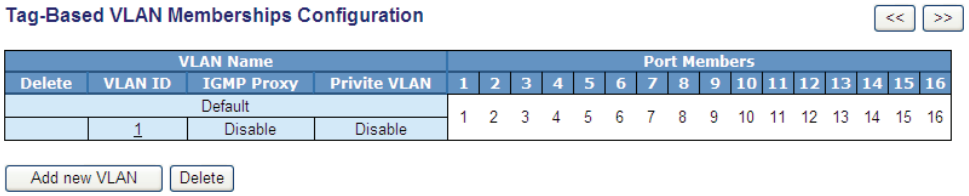


Fig. 3-18

Parameter description:

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximum length is 15 characters.

VLAN ID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

IGMP Proxy:

IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts. This switch can set the IGMP function **"Enable" or "Disable"** by VLAN group. If the VLAN group IGMP proxy is disabled, the switch will stop the exchange of IGMP messages in the VLAN group members. If the VLAN group IGMP proxy is enabled, the switch will support the exchange of IGMP messages in the VLAN group members and follow the IGMP proxy router port configuration, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP. You enable IGMP on the interfaces that connect the system to its hosts that are farther away from the root of the tree. These interfaces are known as downstream interfaces. Please refer to 3-15-1 for detail IGMP Proxy function description.

Member Port:

This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Add new VLAN:

Please click on **<Add new VLAN>** to create a new Tag-based VLAN. Input the VLAN name as well as VID, configure the SYM-VLAN function and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting take effect.

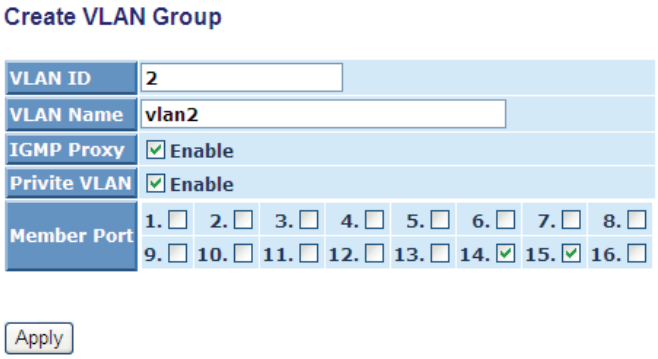


Fig. 3-19

Delete Group:

Just press the **<Delete>** button to remove the selected group entry from the Tag-based group table.

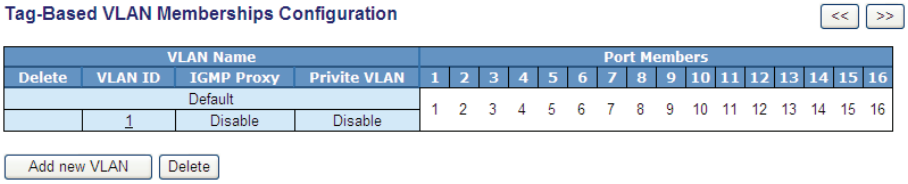


Fig. 3-20

Note: To use the PVLAN (Private VLAN) function, follow the process as below:

a. Create a VLAN as primary VLAN and the VLAN ID is 2 and evoke the Private VLAN to enable Private VLAN service.
b. Assign port member to the VLAN2

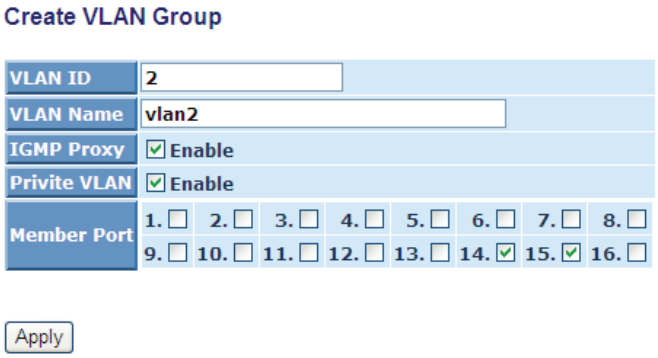


Fig. 3-20-1

c. You need to assign these ports for members of port isolation.

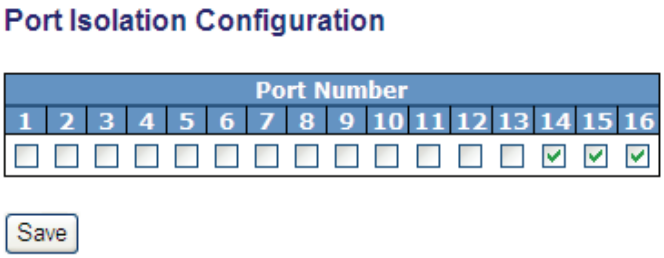


Fig. 3-20-2

d. Press the **"Save"** to complete the PVLAN configuration process.

3-3-3. Port-based Group

Function name:

Port-based Group Configuration

Function description:

It shows the information of the existing Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name.

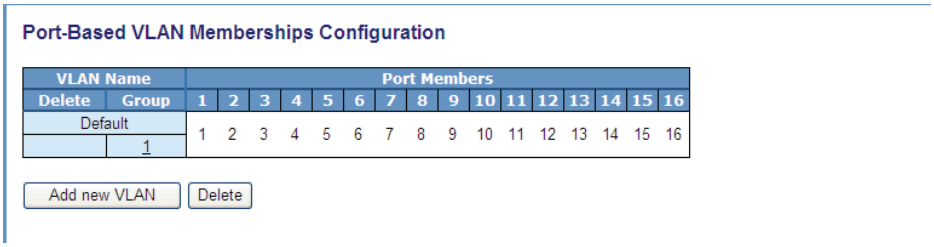

Port-Based VLAN Memberships Configuration
VLAN Name
Port Members
Delete
Group
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Default
1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Add new VLAN
Delete

Fig. 3-21

Parameter description:

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximum length is 15 characters.

Member Port:

This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Add new VLAN:

Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting take effect.

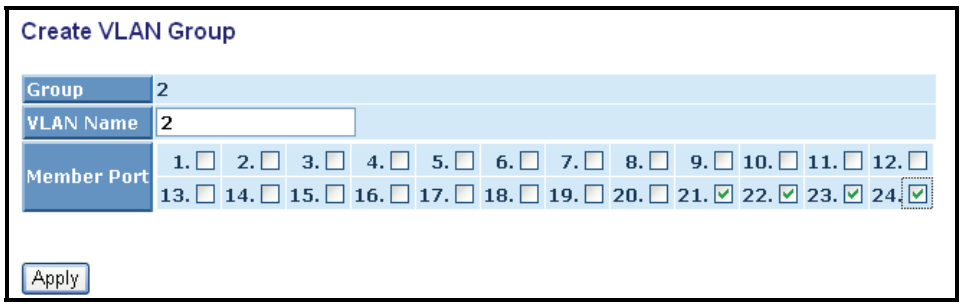


Fig. 3-22

Delete Group:

Just press the **<Delete>** button to remove the selected group entry from the Port-based group table.

Port-Based VLAN Memberships Configuration

VLAN Name		Port Members															
Delete	Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Default		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	1																

Add new VLAN | Delete

Fig. 3-23

3-3-4. Ports

Function name:

VLAN Port Configuration

Function description:

In VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.

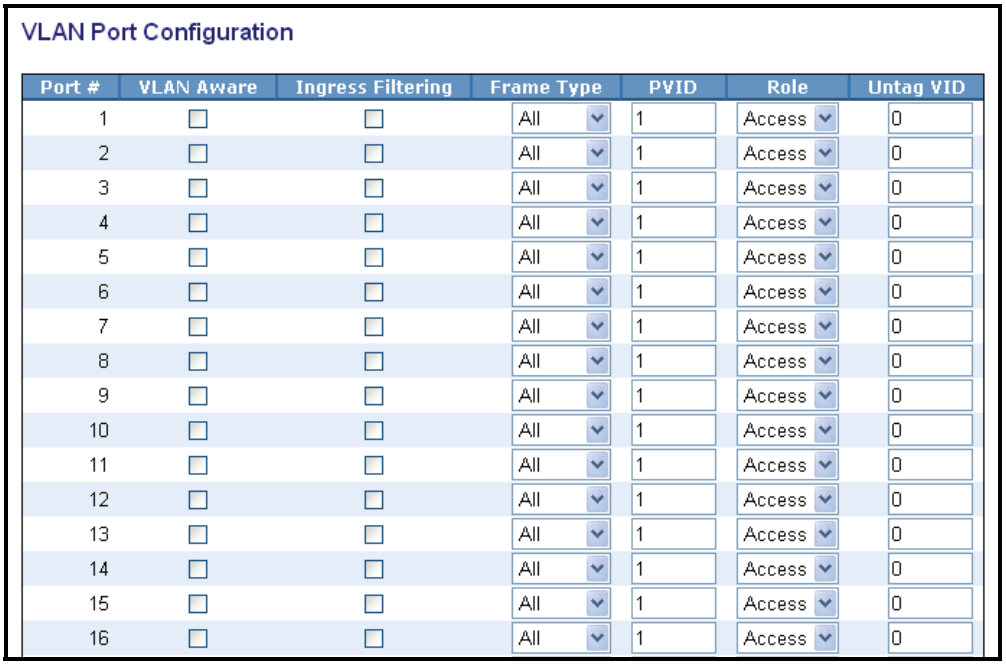

VLAN Port Configuration
Port # VLAN Aware Ingress Filtering Frame Type PVID Role Untag VID
1 All 1 Access 0
2 All 1 Access 0
3 All 1 Access 0
4 All 1 Access 0
5 All 1 Access 0
6 All 1 Access 0
7 All 1 Access 0
8 All 1 Access 0
9 All 1 Access 0
10 All 1 Access 0
11 All 1 Access 0
12 All 1 Access 0
13 All 1 Access 0
14 All 1 Access 0
15 All 1 Access 0
16 All 1 Access 0

Fig. 3-24

Parameter description:

Port 1-16:

Port number.

VLAN Aware:

Based on IEEE 802.1Q VLAN tag to forward packet

Ingress Filtering:

Discard other VLAN group packets, only forward this port’s VLAN group packets

Frame Type:

All: Forward all tagged and untagged packets

Tagged: Forward tagged packets only and discard untagged packets

PVID:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Role:

This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means

the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 1~4094. It works only when Role is set to Hybrid.

3-3-5. Management

Function name:

Management

Function description:

To assign a specific VLAN for management purpose.

Fig. 3-25

Parameter description:

VID: Specific Management VLAN ID.

3-4. MAC

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

3-4-1. Mac Address Table

Function name:

MAC Address Table Information

Function Description:

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.

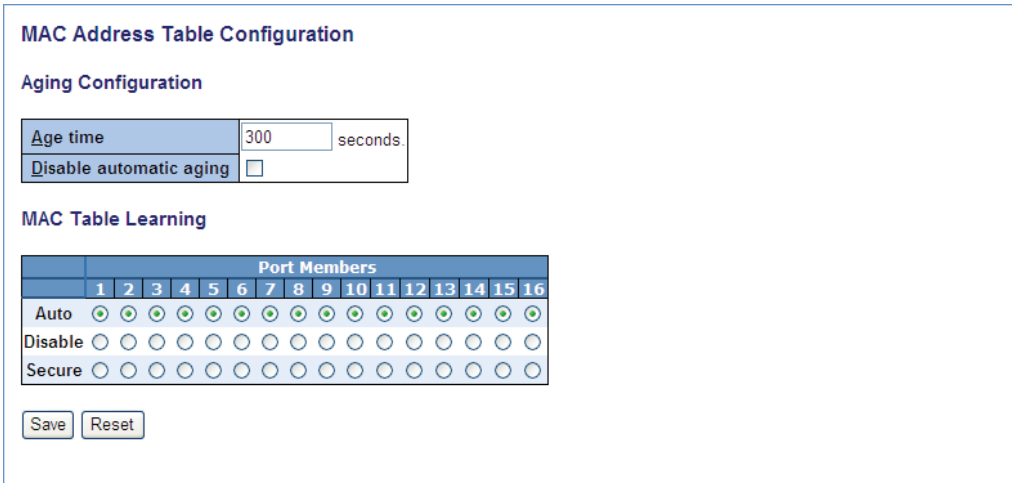


Fig. 3-26

Parameter description:

Aging Time:

Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

Disable automatic aging:

Stop the MAC table aging timer, the learned MAC address will not age out automatically

Auto:

Enable this port's MAC address dynamic learning mechanism.

Disable:

Disable this port's MAC address dynamic learning mechanism, only support static MAC address setting.

Secure:

Disable this port's MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU

Save:

Save MAC Address Table configuration

Reset:

Reset MAC Address Table configuration

3-4-2. Static Filter

Function name:

Static Filter

Function Description:

Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. User can very easily maintain the table by filling in MAC Address, VID (VLAN ID) and Alias fields individually. User also can delete the existing entry by clicking **<Delete>** button.

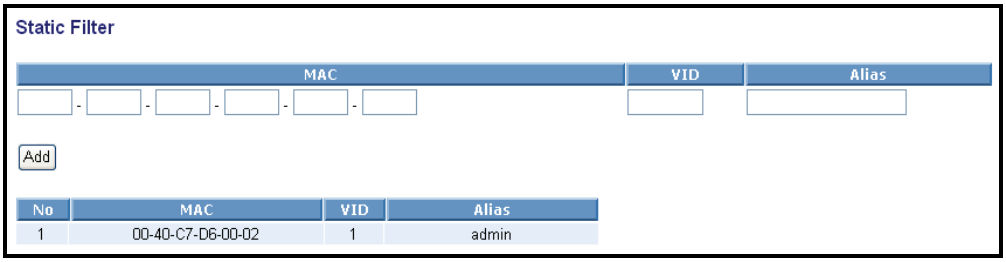


Fig. 3-27

Parameter description:

MAC:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 02

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name you assign.

3-4-3. Static Forward

Function Name:

Static Forward

Function Description:

Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. Static Forward table associated with a specified port of a switch is set up by manually inputting MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffic sent to this MAC address will be forwarded to this port.

For adding a MAC address entry in the allowed table, you just need to fill in four parameters: MAC address, associated port, VID and Alias. Just select the existing MAC address entry you want and click **<Delete>** button.

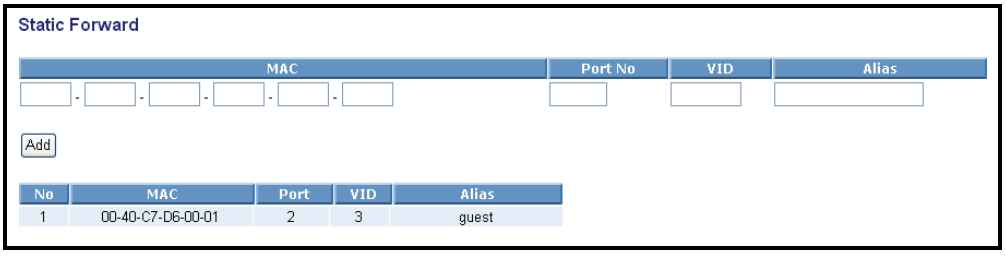


Fig. 3-28

Parameter description:

MAC:

It is a six-byte long Ethernet hardware address usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. It is 1 ~16.

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name you assign.

3-4-4. MAC Alias

Function name:

MAC Alias

Function description:

MAC Alias function is used to let you assign MAC addresses a plain English name. This will help you tell which MAC address belongs to which user. At the initial time, it shows all pairs of the existing alias names and MAC addresses.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click **<Create/Edit>** button to add/modify a new or an existing alias name for a specified MAC address, or mark an existing entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximum length of 15 characters.

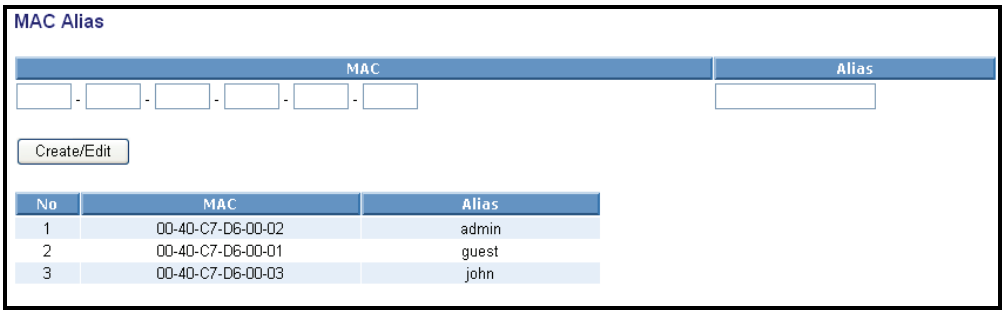


Fig. 3-29

Parameter description:

MAC Address:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Alias:

MAC alias name you assign.

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

3-4-5. MAC Table

Function name:

Dynamic MAC Table

Function Description:

Displays the static or dynamic learning MAC entry and the state for the selected port.

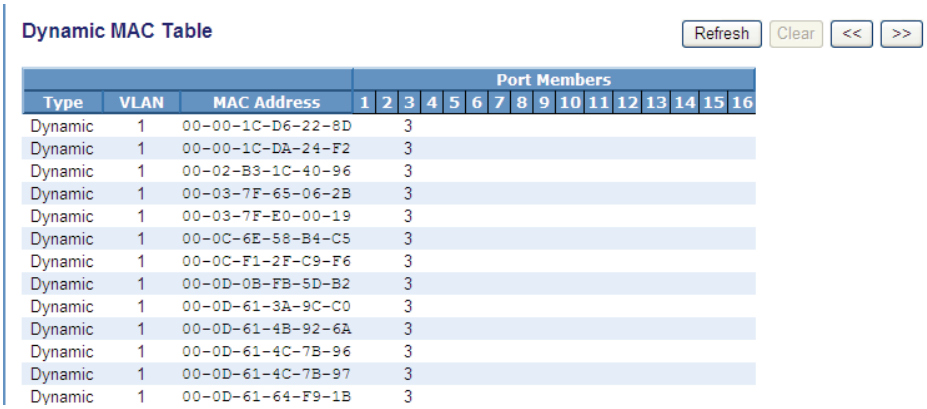

Dynamic MAC Table
Refresh
Clear
<<
>>
Port Members
Type VLAN MAC Address 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Dynamic 1 00-00-1C-D6-22-8D 3
Dynamic 1 00-00-1C-DA-24-F2 3
Dynamic 1 00-02-B3-1C-40-96 3
Dynamic 1 00-03-7F-65-06-2B 3
Dynamic 1 00-03-7F-E0-00-19 3
Dynamic 1 00-0C-6E-58-B4-C5 3
Dynamic 1 00-0C-F1-2F-C9-F6 3
Dynamic 1 00-0D-0B-FB-5D-B2 3
Dynamic 1 00-0D-61-3A-9C-C0 3
Dynamic 1 00-0D-61-4B-92-6A 3
Dynamic 1 00-0D-61-4C-7B-96 3
Dynamic 1 00-0D-61-4C-7B-97 3
Dynamic 1 00-0D-61-64-F9-1B 3

Fig. 3-30

Parameter description:

Type:

Dynamic or Static.

VLAN:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

MAC address:

Displays the MAC address of one entry you selected from the searched MAC entries table.

Port:

The port that exists in the searched MAC Entry.

Refresh:

Refresh function can help you to see current MAC Table status.

Clear:

To clear the selected entry.

Previous Page:

Move to the previous page.

Next Page:

Move to the next page.

3-5. GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machines maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate this information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.

3-5-1. Config

Function name:

GVRP Configuration

Function description:

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

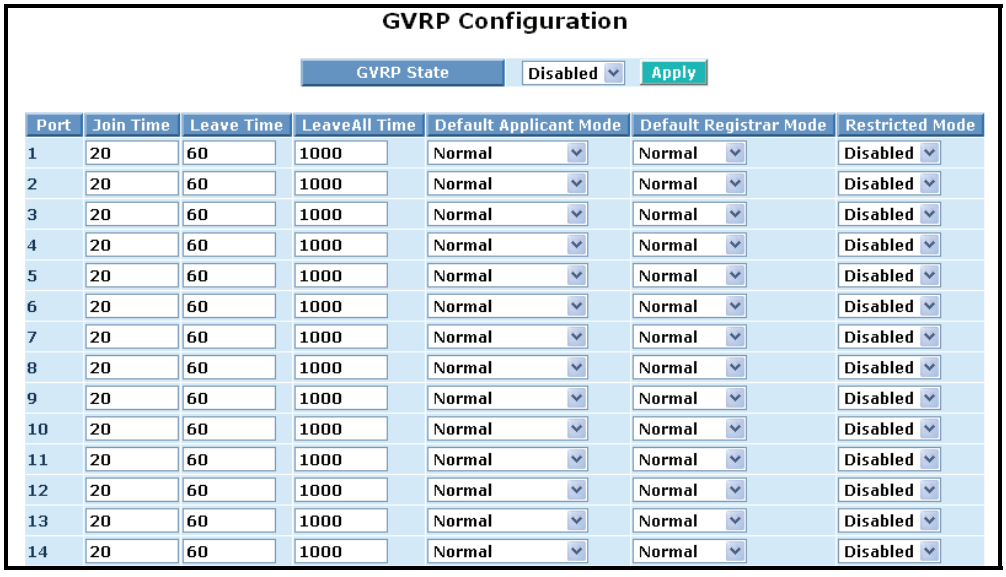

GVRP Configuration
GVRP State
Disabled
Apply
Port
Join Time
Leave Time
LeaveAll Time
Default Applicant Mode
Default Registrar Mode
Restricted Mode
1 20 60 1000 Normal Normal Disabled
2 20 60 1000 Normal Normal Disabled
3 20 60 1000 Normal Normal Disabled
4 20 60 1000 Normal Normal Disabled
5 20 60 1000 Normal Normal Disabled
6 20 60 1000 Normal Normal Disabled
7 20 60 1000 Normal Normal Disabled
8 20 60 1000 Normal Normal Disabled
9 20 60 1000 Normal Normal Disabled
10 20 60 1000 Normal Normal Disabled
11 20 60 1000 Normal Normal Disabled
12 20 60 1000 Normal Normal Disabled
13 20 60 1000 Normal Normal Disabled
14 20 60 1000 Normal Normal Disabled

Fig. 3-31

Parameter description:

GVRP State:

This function is simply to let you enable or disable GVRP function. You can pull down the list and click the **<Downward>** arrow key to choose “Enable” or “Disable”. Then, click the **<Apply>** button, the system will take effect immediately.

Join Time:

Used to declare the Join Time in unit of centisecond. Valid time range: 20 –100 centisecond, Default: 20 centisecond.

Leave Time:

Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.

Leave All Time:

A time period for announcement that all registered devices are going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

Default Applicant Mode:

The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user’s choice.

Normal:

In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant:

In this mode, the switch does not send or reply any GARP messages. It just listens to messages and reacts for the received GVRP BPDU.

Default Registrar Mode:

The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user’s choice.

Normal:

The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed:

The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden:

The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict dynamic VLAN being created when this port receives GVRP PDU. There are two modes, disable and enable, provided for the user’s choice.

Disabled:

In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create dynamic VLAN when this port receives GVRP PDU. Except when it receives a dynamic VLAN message of the GVRP PDU

is an existing static VLAN in the switch, this port will be added into the static VLAN members dynamically.

3-5-2. Counter

Function name:

GVRP Counter

Function description:

All GVRP counters are mainly divided into Received and Transmitted categories to let you monitor the GVRP actions. Actually, they are GARP packets.

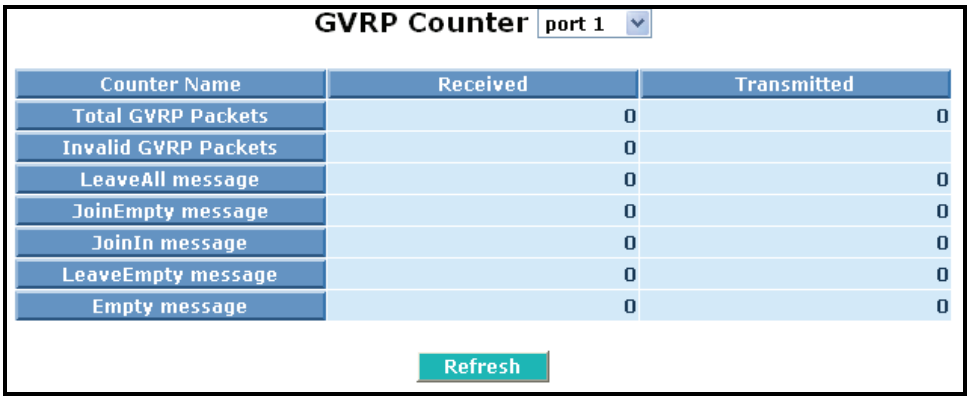


Fig. 3-32

Parameter description:

Received:

Total GVRP Packets:

Total GVRP BPDU is received by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is received by the GARP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is received by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is received by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is received by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is received by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is received by the GARP application.

Transmitted:

Total GVRP Packets:

Total GARP BPDU is transmitted by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is transmitted by the GVRP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is transmitted by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is transmitted by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is transmitted by the GARP application.

3-5-3. Group

Function name:

GVRP Group VLAN Information

Function description:

To show the dynamic group member and their information.

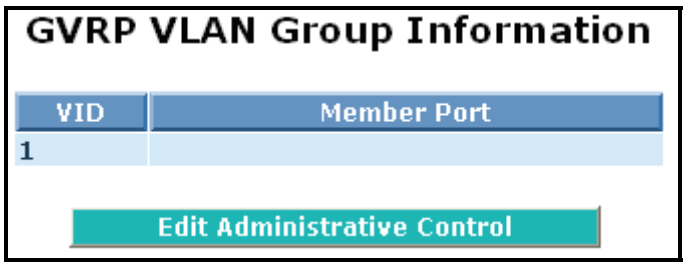


Fig. 3-33

Parameter description:

VID:

VLAN identifier. When GVRP groups are created, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port:

The members belonging to the same dynamic VLAN group.

Edit Administrative Control:

When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.

3-6. QoS(Quality of Service) Configuration

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms providing excellent performance for all QoS classes under any traffic scenario, including jumbo frame. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

3-6-1. Ports

Function name:

Port QoS Configuration

Function description:

To configure each port QoS behavior. Four QoS queue per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

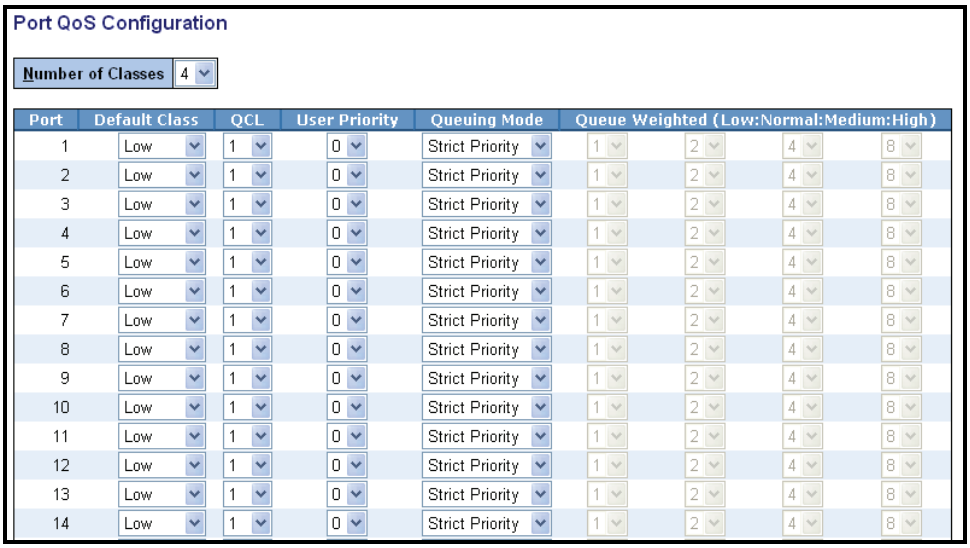

Port QoS Configuration
Number of Classes 4
Port Default Class QCL User Priority Queuing Mode Queue Weighted (Low:Normal:Medium:High)
1 Low 1 0 Strict Priority 1 2 4 8
2 Low 1 0 Strict Priority 1 2 4 8
3 Low 1 0 Strict Priority 1 2 4 8
4 Low 1 0 Strict Priority 1 2 4 8
5 Low 1 0 Strict Priority 1 2 4 8
6 Low 1 0 Strict Priority 1 2 4 8
7 Low 1 0 Strict Priority 1 2 4 8
8 Low 1 0 Strict Priority 1 2 4 8
9 Low 1 0 Strict Priority 1 2 4 8
10 Low 1 0 Strict Priority 1 2 4 8
11 Low 1 0 Strict Priority 1 2 4 8
12 Low 1 0 Strict Priority 1 2 4 8
13 Low 1 0 Strict Priority 1 2 4 8
14 Low 1 0 Strict Priority 1 2 4 8

Fig. 3-34

Parameter description:

Number of Classes:

1 / 2 / 4

Port:

User can choose the port (1~16) respectively with Priority Class on Per Port Priority function.

Default Class:

User can set up High Priority or Low Priority for each port respectively.

Low / Normal / Medium / High

QCL:

The number of QCL rule 1~24, each port has to apply one of the QCL rules for QoS behavior

User priority:

The user priority value 0~7 (3 bits) is used as an index to the eight QoS class values for VLAN tagged or priority tagged frames.

Queuing Mode:

There are two Scheduling Methods, Strict Priority and Weighted Fair. Default is Strict Priority. After you choose any Scheduling Method, please click Apply button.

Queue Weighted:

There are four queues per port and four classes, weighted number (1 / 2 / 4 / 8) for each queue, you can select the weighted number when the scheduling method is set to “Weighted Fair” mode.

3-6-2. Qos Control List

Function name:

Qos Control List Configuration

Function description:

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ether Type, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

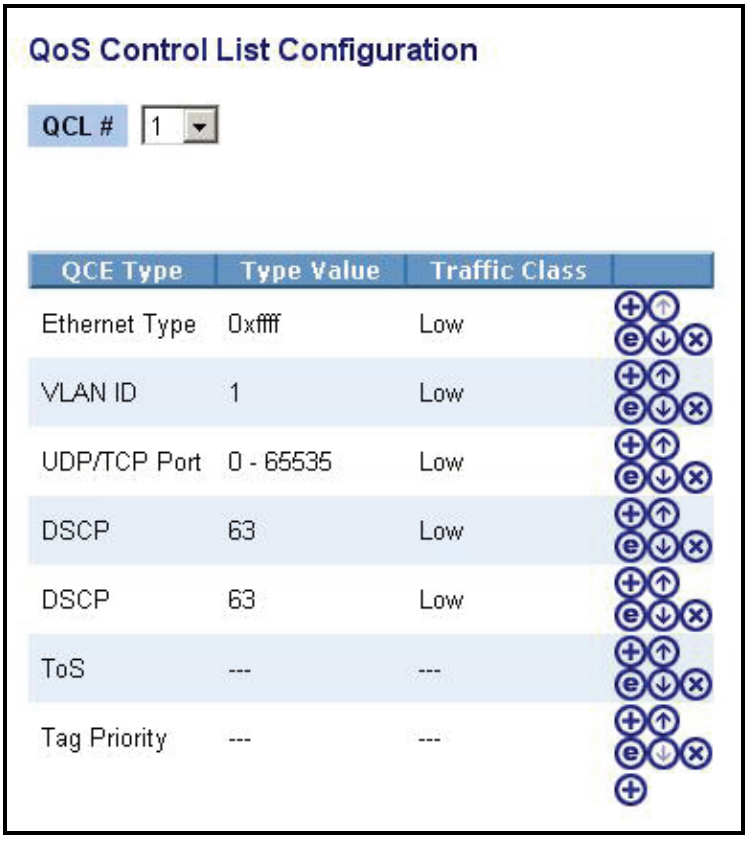
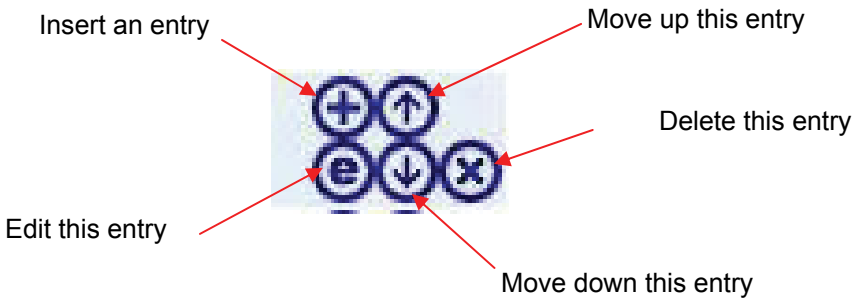


Fig. 3-35



QCE Configuration:

The QCL consists of 12 QoS Control Entries (QCEs) that are searched from the top of the list to the bottom of the list for a match. The first matching QCE determines the QoS classification of the frame. The QCE ordering is therefore important for the resulting QoS classification algorithm. If no matching QCE is found, the default QoS class is used in the port QoS configuration.

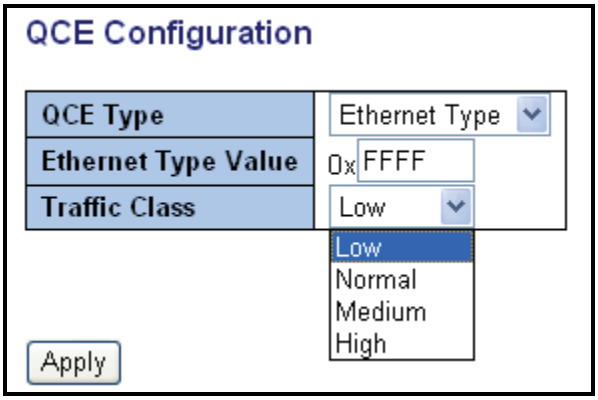


Fig. 3-36

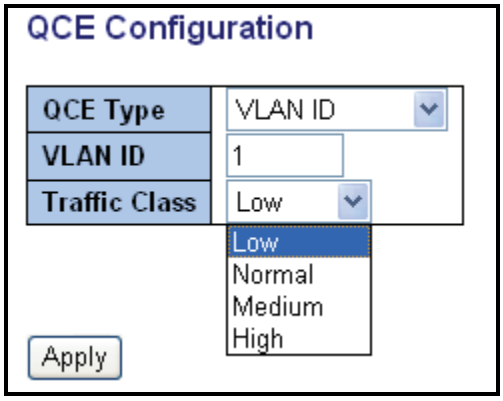


Fig. 3-37

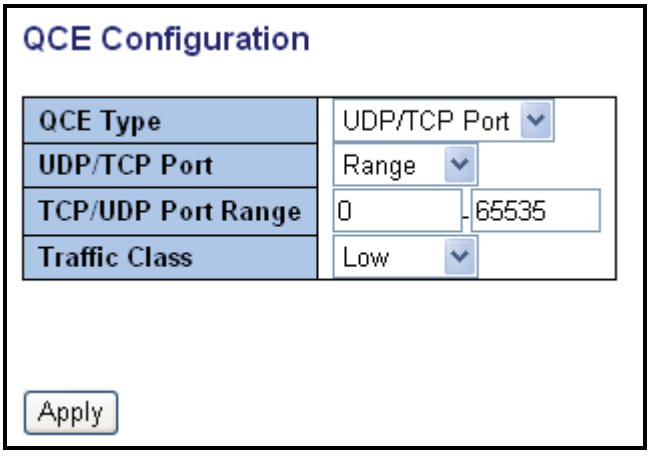


Fig. 3-38

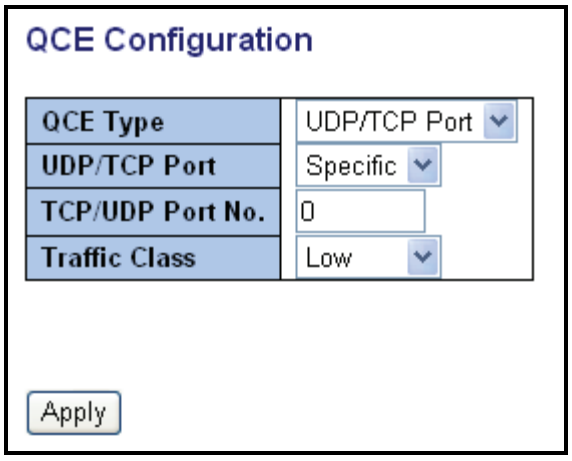


Fig. 3-39

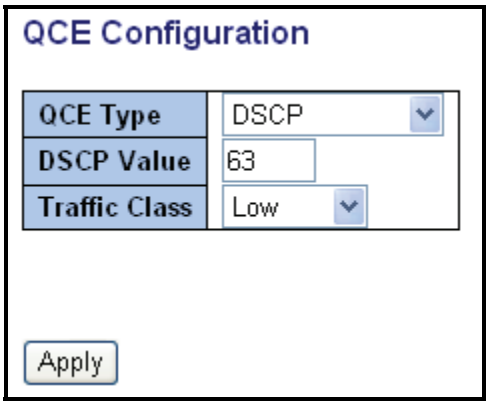


Fig. 3-40

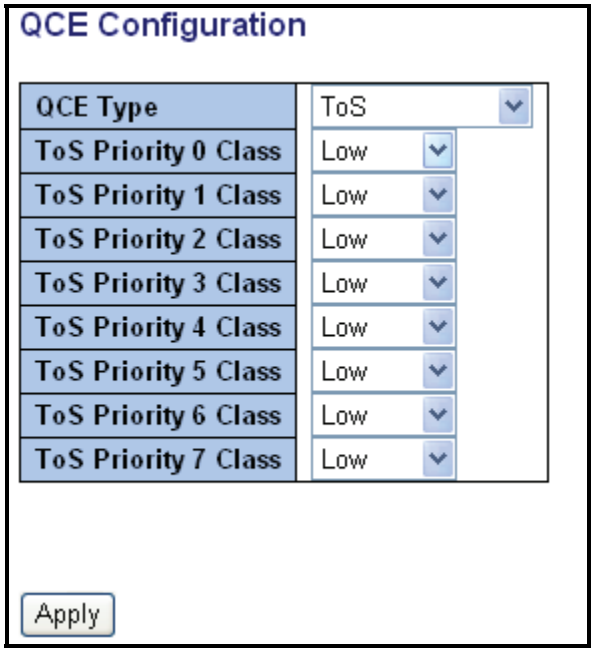


Fig. 3-41

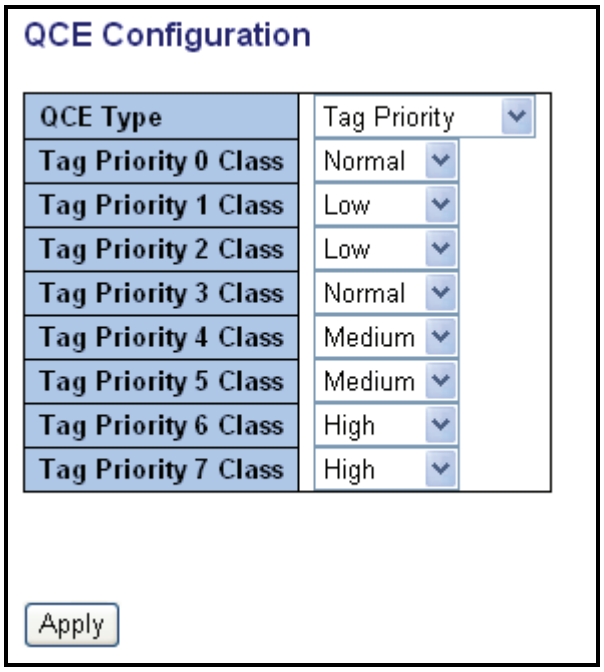


Fig. 3-42

Parameter description:

QCL#:

QCL number : 1~24

QCE Type:

Ethernet Type / VLAN ID / UDP/TCP Port / DSCP / ToS / Tag Priority

Ethernet Type Value:

The configurable range is 0x600~0xFFFF. Well known protocols are already assigned EtherType values. The commonly used values in the EtherType field and corresponding protocols are listed below:

Ethertype (Hexadecimal)	Protocol
0x0800	IP, Internet Protocol
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP, Address Resolution Protocol.
0x0808	Frame Relay ARP [RFC1701]
0x6559	Raw Frame Relay [RFC1701]
0x8035	DRARP, Dynamic RARP. RARP, Reverse Address Resolution Protocol.
0x8037	Novell Netware IPX
0x809B	EtherTalk (AppleTalk over Ethernet)

0x80D5	IBM SNA Services over Ethernet
0x 80F3	AARP, AppleTalk Address Resolution Protocol.
0x8100	IEEE Std 802.1Q - Customer VLAN Tag Type.
0x8137	IPX, Internet Packet Exchange.
0x 814C	SNMP, Simple Network Management Protocol.
0x86DD	IPv6, Internet Protocol version 6.
0x880B	PPP, Point-to-Point Protocol.
0x 880C	GSMP, General Switch Management Protocol.
0x8847	MPLS, Multi-Protocol Label Switching (unicast).
0x8848	MPLS, Multi-Protocol Label Switching (multicast).
0x8863	PPPoE, PPP Over Ethernet (Discovery Stage).
0x8864	PPPoE, PPP Over Ethernet (PPP Session Stage).
0x88BB	LWAPP, Light Weight Access Point Protocol.
0x88CC	LLDP, Link Layer Discovery Protocol.
0x8E88	EAPOL, EAP over LAN.
0x9000	Loopback (Configuration Test Protocol)
0xFFFF	reserved.

VLAN ID:

The configurable VID range:1~4094

UDP/TCP Port:

To select the UDP/TCP port classification method by Range or Specific.

UDP/TCP Port Range:

The configurable ports range: 0~65535
You can refer to following UDP/TCP port-numbers information.
http://www.iana.org/assignments/port-numbers

UDP/TCP Port No.:

The configurable specific port value: 0~65535

DSCP Value:

The configurable DSCP value: 0~63

Traffic Class:

Low / Normal / Medium / High

3-6-3.Rate Limiters

Function name:

Rate Limit Configuration

Function description:

Each port includes an ingress policer, and an egress shaper, which can limit the bandwidth of received and transmitted frames. Ingress policer or egress shaper operation is controlled per port in the Rate Limit Configuration.

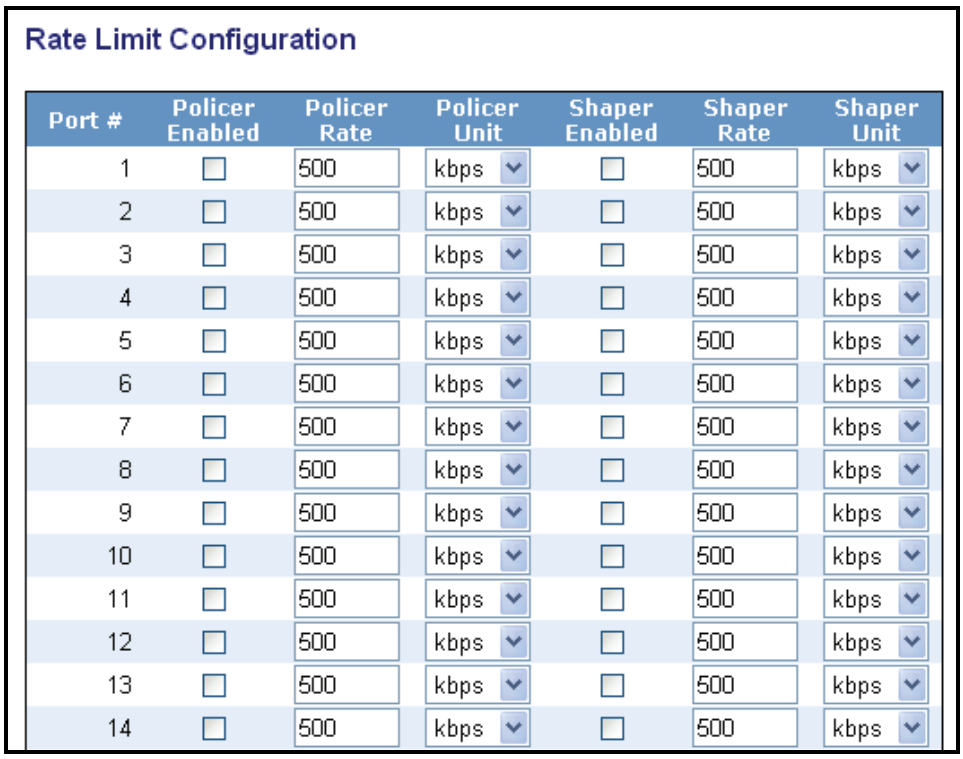

Rate Limit Configuration
Port #
Policer Enabled
Policer Rate
Policer Unit
Shaper Enabled
Shaper Rate
Shaper Unit
1 500 kbps 500 kbps
2 500 kbps 500 kbps
3 500 kbps 500 kbps
4 500 kbps 500 kbps
5 500 kbps 500 kbps
6 500 kbps 500 kbps
7 500 kbps 500 kbps
8 500 kbps 500 kbps
9 500 kbps 500 kbps
10 500 kbps 500 kbps
11 500 kbps 500 kbps
12 500 kbps 500 kbps
13 500 kbps 500 kbps
14 500 kbps 500 kbps

Fig. 3-43

Parameter description:

Port #:

Port number.

Policer Enabled:

Policer enabled to limit ingress bandwidth by policer rate.

Policer Rate:

The configurable policer rate range:
500 Kbps ~ 1000000 Kbps
1 Mbps ~ 1000 Mbps

Policer Unit:

There are two units for ingress policer rate limit: kbps / Mbps

Shaper Enabled:

Shaper enabled to limit egress bandwidth by shaper rate.

Shaper Rate:

The configurable shaper rate range:
500 Kbps ~ 1000000 Kbps
1 Mbps ~ 1000 Mbps

Shaper Unit:

There are two units for egress shaper rate limit: kbps / Mbps

3-6-4.Storm Control

Function name:

Storm Control Configuration

Function description:

The switch supports storm ingress policer control function to limit the Flooded, Multicast and Broadcast to prevent storm event happen.

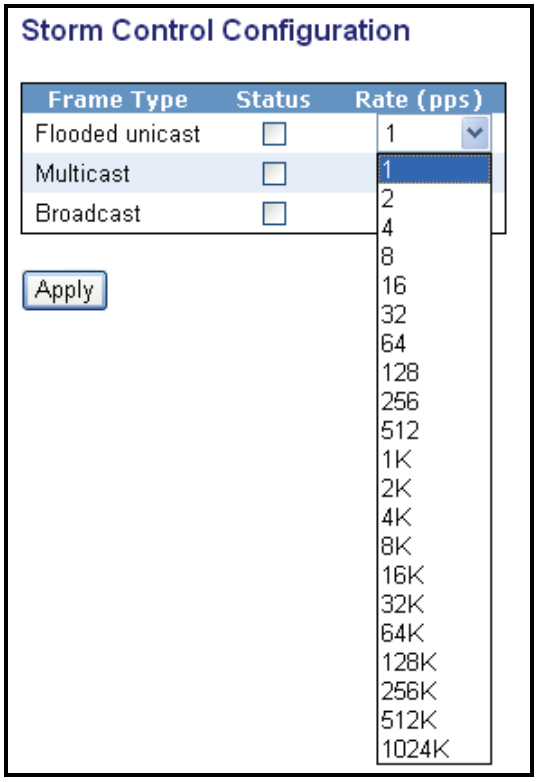


Fig. 3-44

Parameter description:

Frame Type:

There are three frame types of storm that can be controlled: Flooded unicast / Multicast / Broadcast

Status:

Enable/Disable Selection: ☑ means enabled, ☐ means disabled

Rate(pps):

Refer to the following rate configurable value list, the unit is Packet Per Second (pps).

1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

3-6-5.Wizard

Function name:

Wizard

Function description:

The QCL configuration Wizard is targeted so the user can easily configure the QCL rules for QoS configuration. The wizard provides the typical network application rules. The user can apply these applications easily.

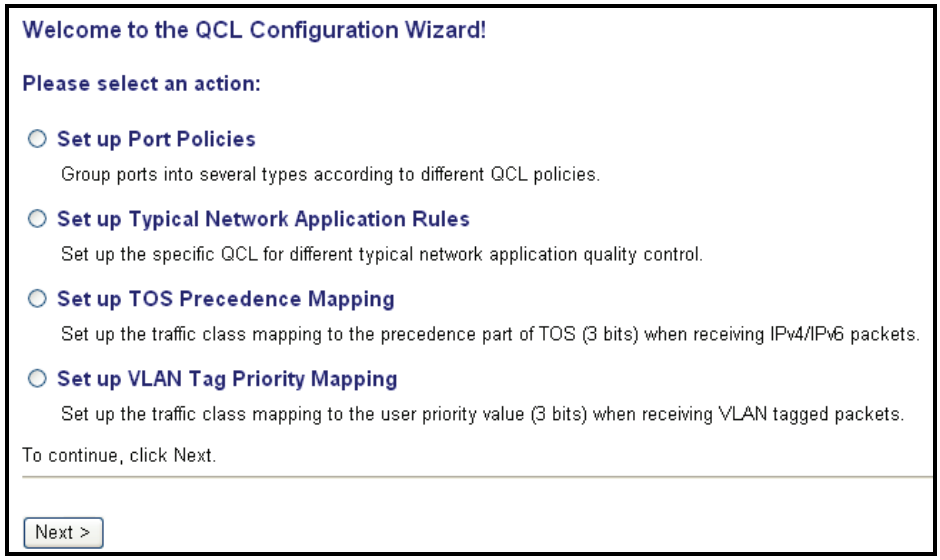

Welcome to the QCL Configuration Wizard!
Please select an action:
Set up Port Policies
Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control.
Set up TOS Precedence Mapping
Set up the traffic class mapping to the precedence part of TOS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.
To continue, click Next.
Next >

Fig. 3-45

Parameter description:

Please select an Action:

User needs to select one action from the following items, then click on **<Next>** to finish QCL configuration:

- Set up Port Policies
- Set up Typical Network Application Rules
- Set up TOS Precedence Mapping
- Set up VLAN Tag Priority Mapping

Next:

Go to next step.

Cancel:

Abort current configuration back to previous step.

Back:

Back to previous screen.

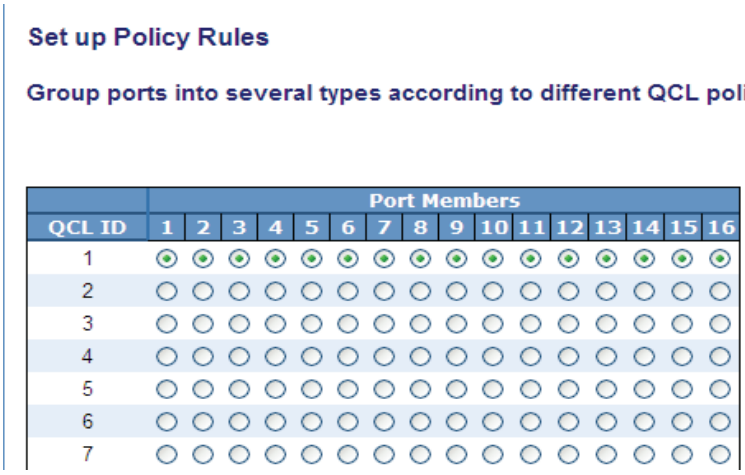


Fig. 3-46 Set up Port Policies

Parameter description:

QCL ID:

QoS Control List (QCL): 1~24

Port Member:

Port Member: 1~16

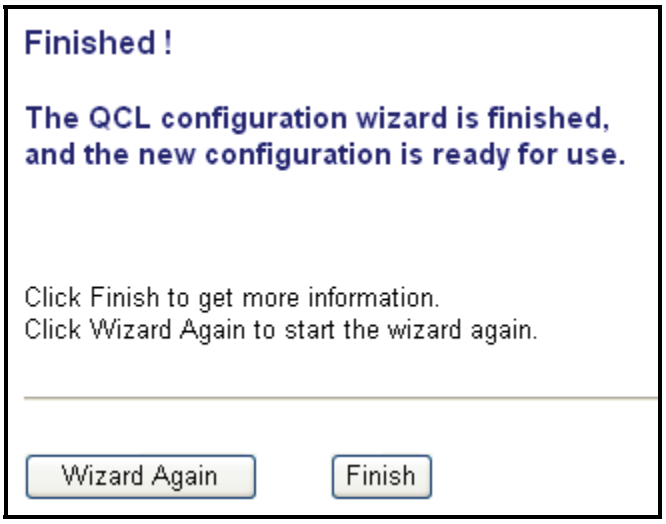

Finished !
The QCL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-47 Set up Port Policies

Parameter description:

Wizard Again:

Click on the <Wizard Again>, back to QCL Configuration Wizard.

Finish:

When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen. Click on <Apply> for changed parameters confirmation.

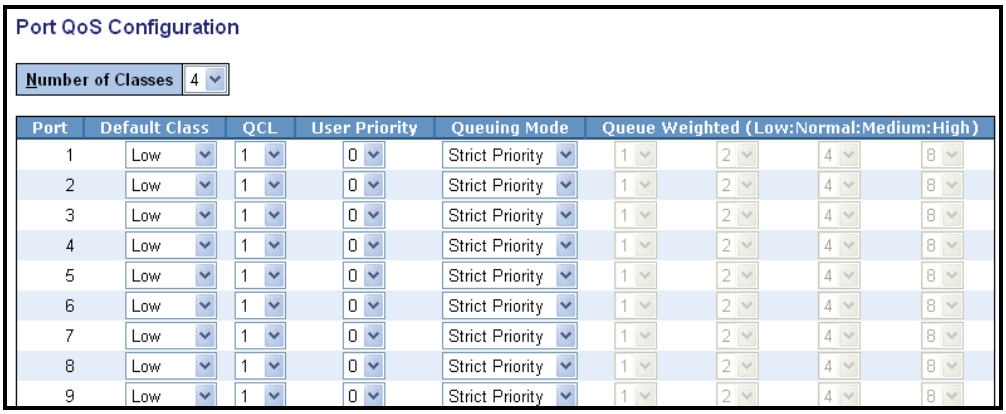

Port QoS Configuration
Number of Classes 4
Port Default Class QCL User Priority Queuing Mode Queue Weighted (Low:Normal:Medium:High)
1 Low 1 0 Strict Priority 1 2 4 8
2 Low 1 0 Strict Priority 1 2 4 8
3 Low 1 0 Strict Priority 1 2 4 8
4 Low 1 0 Strict Priority 1 2 4 8
5 Low 1 0 Strict Priority 1 2 4 8
6 Low 1 0 Strict Priority 1 2 4 8
7 Low 1 0 Strict Priority 1 2 4 8
8 Low 1 0 Strict Priority 1 2 4 8
9 Low 1 0 Strict Priority 1 2 4 8

Fig. 3-48 Set up Port Policies Finish

Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control by selecting the network application type for your rule:
o Audio and Video
QuickTime 4 Server MSN Messenger Phone Yahoo Messenger Phone Napster Real Audio
o Games
Blizzard Battlenet (Diablo2 and StarCraft) Fighter Ace II Quake2 Quake3 MSN Game Zone
o User Definition
Ethernet Type VLAN ID UDP/TCP Port DSCP

Fig. 3-49 Set up Typical Network Application Rules

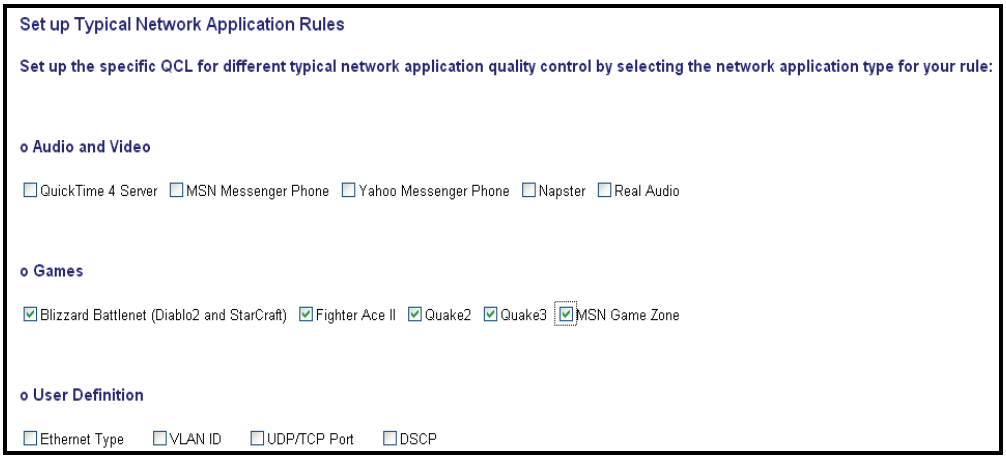

Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control by selecting the network application type for your rule:
o Audio and Video
QuickTime 4 Server MSN Messenger Phone Yahoo Messenger Phone Napster Real Audio
o Games
Blizzard Battlenet (Diablo2 and StarCraft) Fighter Ace II Quake2 Quake3 MSN Game Zone
o User Definition
Ethernet Type VLAN ID UDP/TCP Port DSCP

Fig. 3-50 Set up Typical Network Application Rules

Fig. 3-51 Set up Typical Network Application Rules

Parameter description:

Audio and Video:

QuickTime 4 Server / MSN Messenger Phone / Yahoo Messenger Phone / Napster / Real Audio

Games:

Blizzard Battlenet (Diablo2 and StarCraft) / Fighter Ace II / Quake2 / Quake3 / MSN Game Zone

User Definition:

Ethernet Type / VLAN ID / UDP/TCP Port / DSCP

Ethernet Type Value:

Type Range: 0x600~0xFFFF

VLAN ID:

VLAN ID Range: 1~4094

UDP/TCP Port:

Two Mode: Range / Specific

UDP/TCP Port Range:

Port Range: 0~65535

UDP/TCP Port No.:

Port Range: 0~65535

DSCP Value:

DSCP Value Range: 0~63

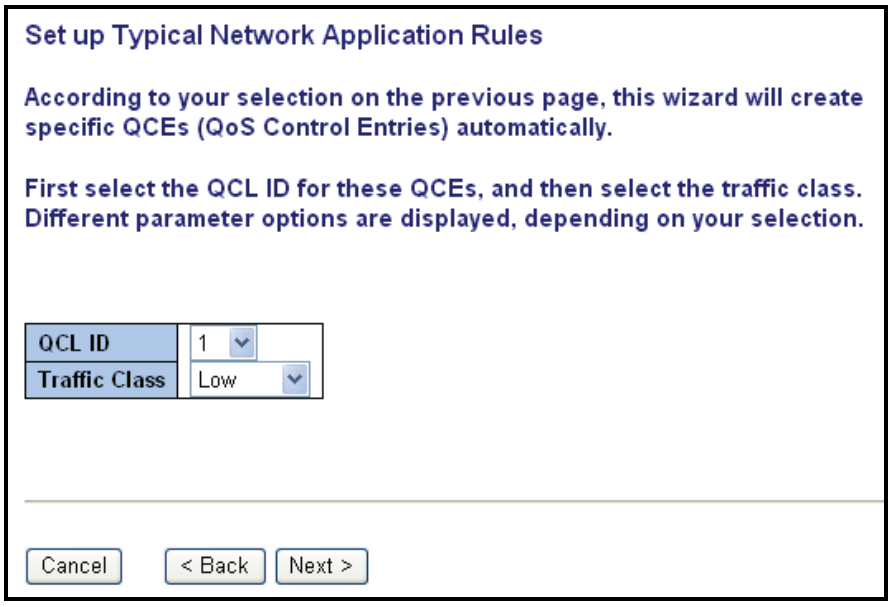

Set up Typical Network Application Rules
According to your selection on the previous page, this wizard will create specific QCEs (QoS Control Entries) automatically.
First select the QCL ID for these QCEs, and then select the traffic class. Different parameter options are displayed, depending on your selection.
QCL ID
1
Traffic Class
Low
Cancel
< Back
Next >

Fig. 3-52 Set up Typical Network Application Rules

Parameter description:

QCL ID:

QCL ID Range: 1~24

Traffic Class:

There are four classes: Low / Normal / Medium / High

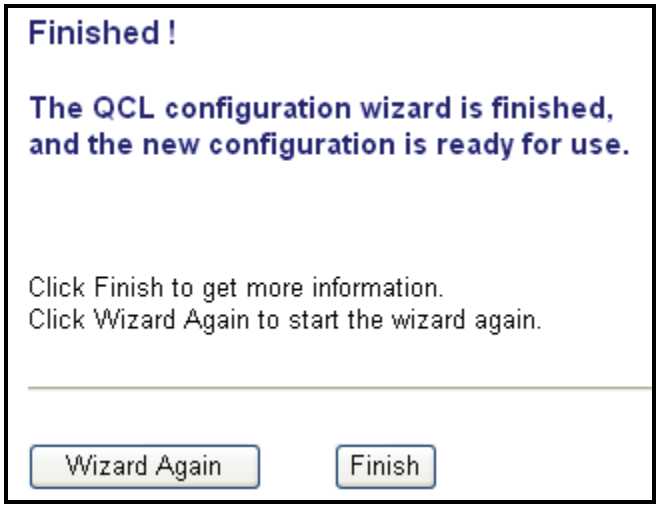

Finished !
The QCL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-53 Set up Typical Network Application Rules

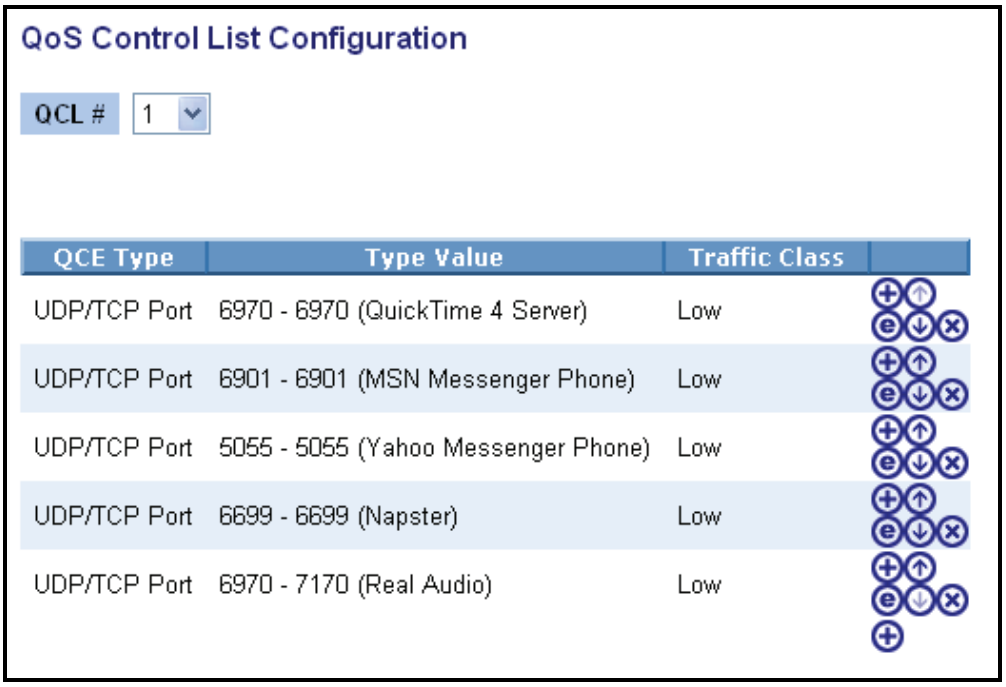

QoS Control List Configuration
QCL # 1
QCE Type
Type Value
Traffic Class
UDP/TCP Port 6970 - 6970 (QuickTime 4 Server) Low
UDP/TCP Port 6901 - 6901 (MSN Messenger Phone) Low
UDP/TCP Port 5055 - 5055 (Yahoo Messenger Phone) Low
UDP/TCP Port 6699 - 6699 (Napster) Low
UDP/TCP Port 6970 - 7170 (Real Audio) Low

Fig. 3-54 Set up Typical Network Application Rules Finish

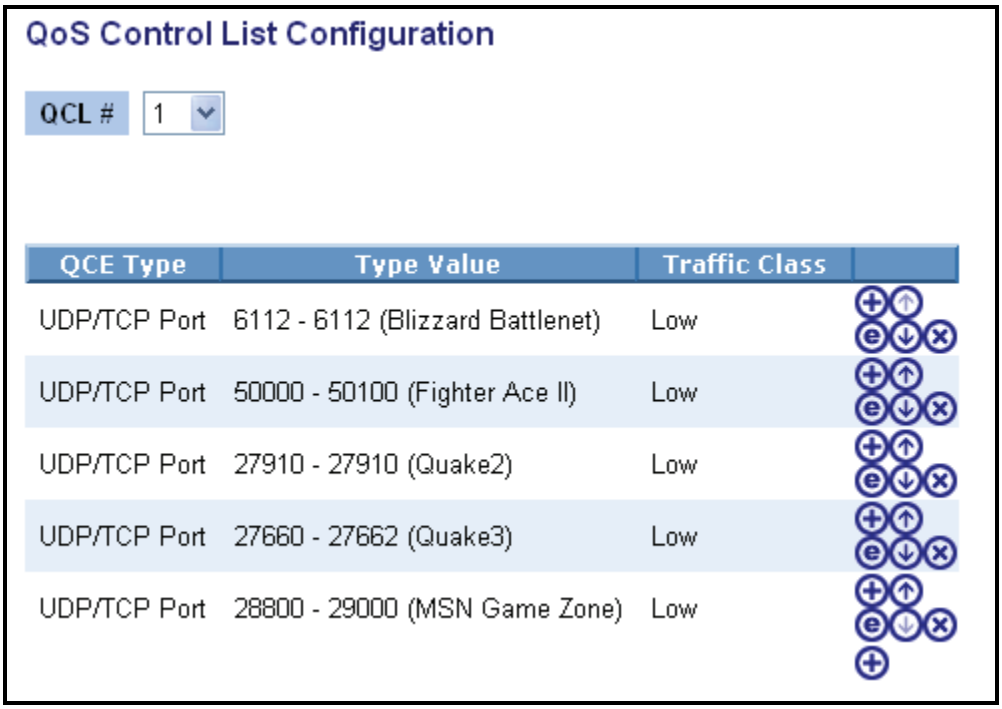

QoS Control List Configuration
QCL # 1
QCE Type
Type Value
Traffic Class
UDP/TCP Port 6112 - 6112 (Blizzard Battlenet) Low
UDP/TCP Port 50000 - 50100 (Fighter Ace II) Low
UDP/TCP Port 27910 - 27910 (Quake2) Low
UDP/TCP Port 27660 - 27662 (Quake3) Low
UDP/TCP Port 28800 - 29000 (MSN Game Zone) Low

Fig. 3-55 Set up Typical Network Application Rules Finish

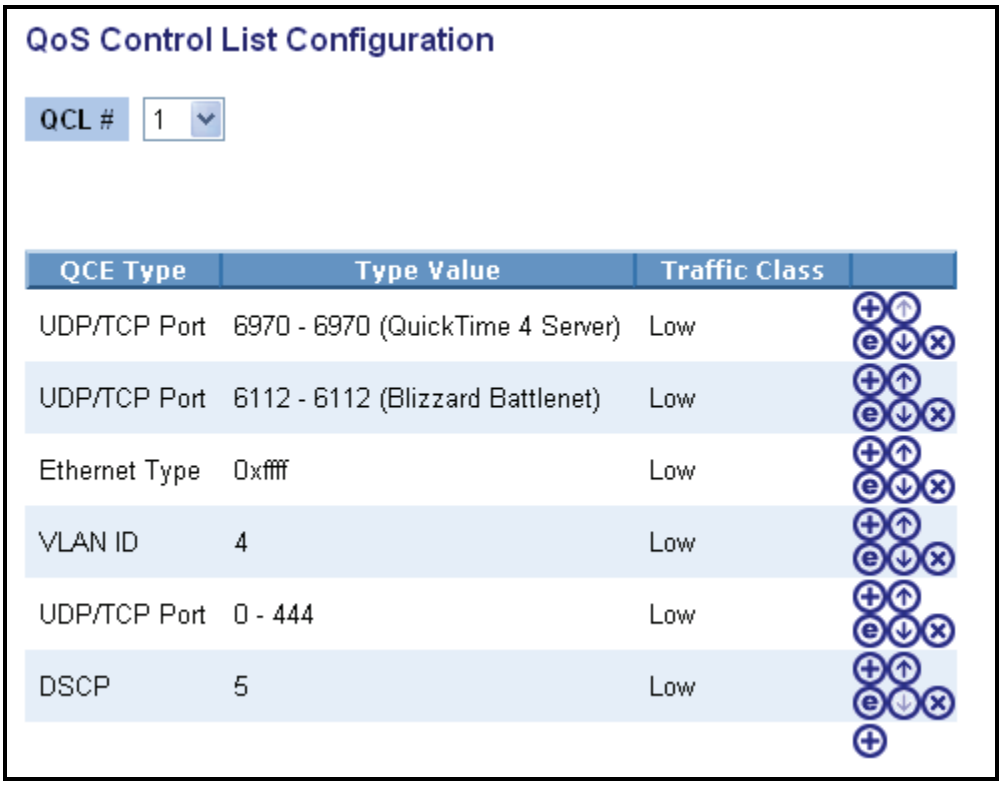


Fig. 3-56 Set up Typical Network Application Rules Finish

Parameter description:

QCL #:

QoS Control List (QCL): 1~24

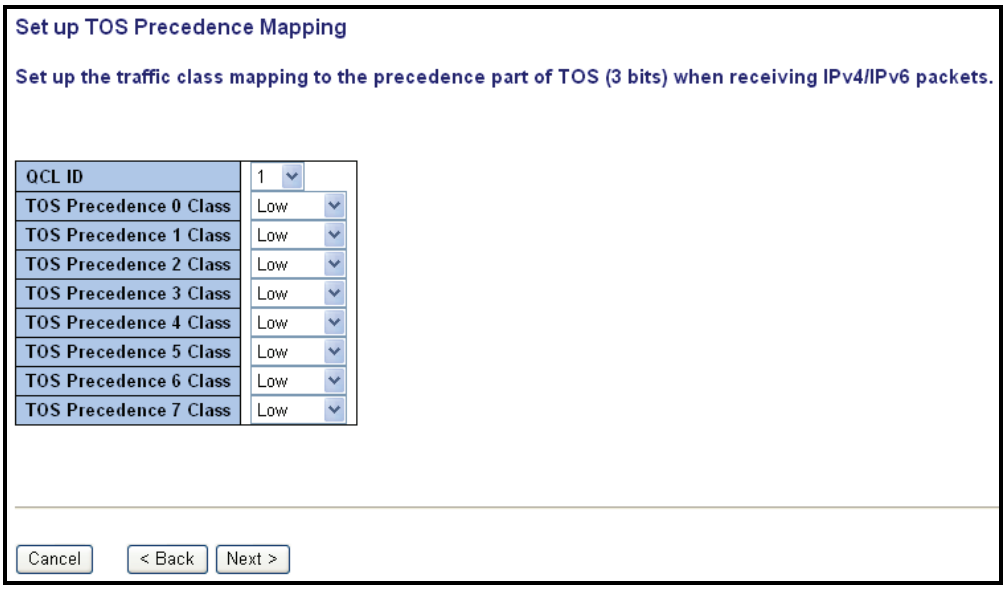


Fig. 3-57 Set up TOS Precedence Mapping

Parameter description:

QCL ID:

QoS Control List (QCL): 1~24

TOS Precedence 0~7 Class:

Low / Normal / Medium / High

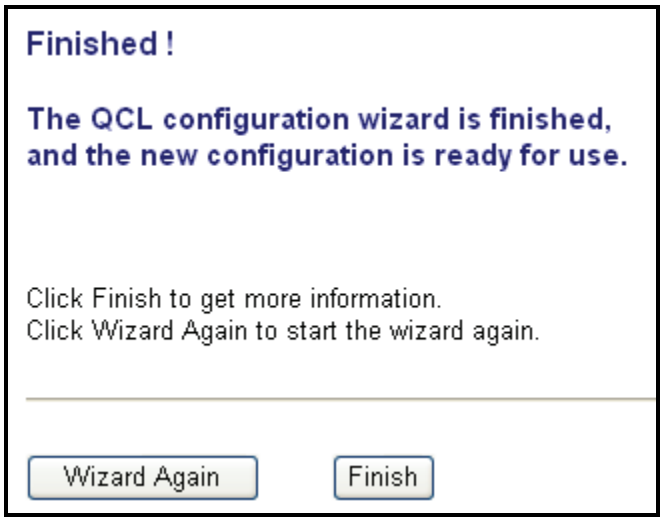

Finished !
The QCL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-58 Set up TOS Precedence Mapping

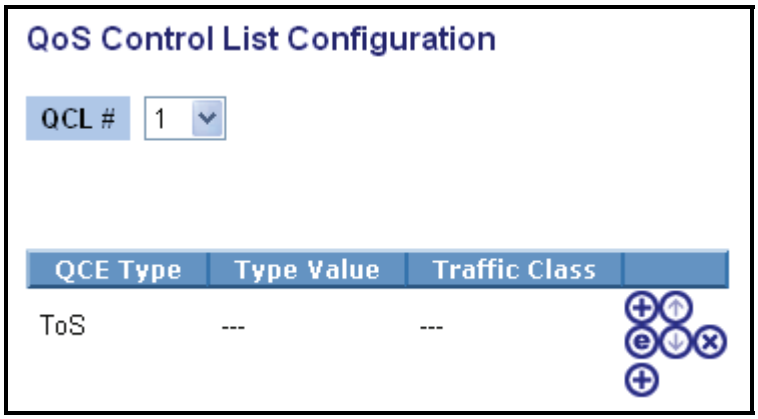


Fig. 3-59 Set up TOS Precedence Mapping Finish

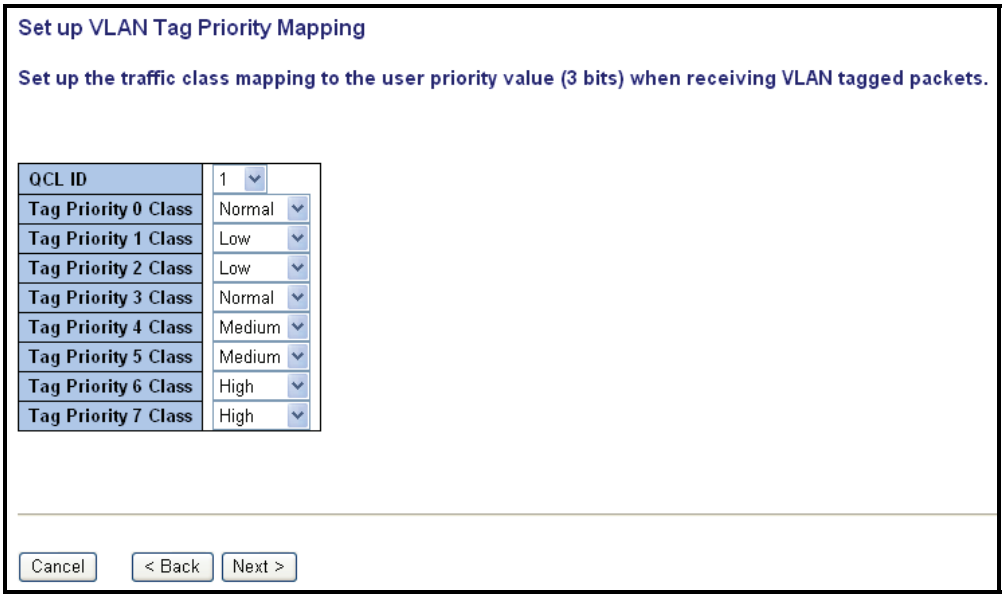


Fig. 3-60 Set up VLAN Tag Priority Mapping

Parameter description:

QCL ID:

QoS Control List (QCL): 1~24

Tag Priority 0~7 Class:

Low / Normal / Medium / High

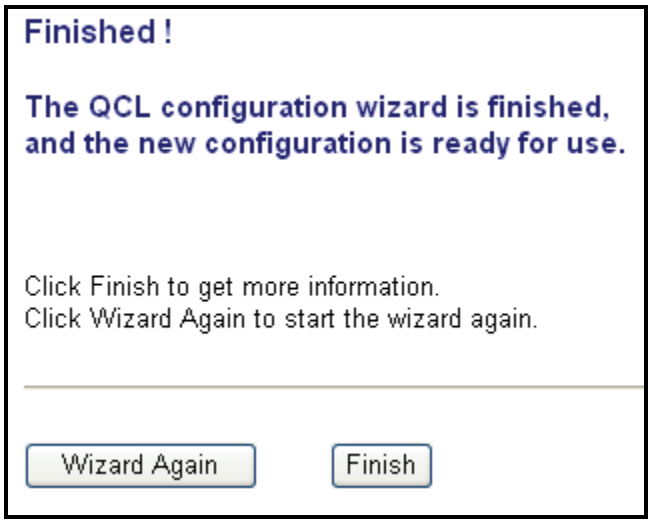

Finished !
The QCL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-61 Set up VLAN Tag Priority Mapping

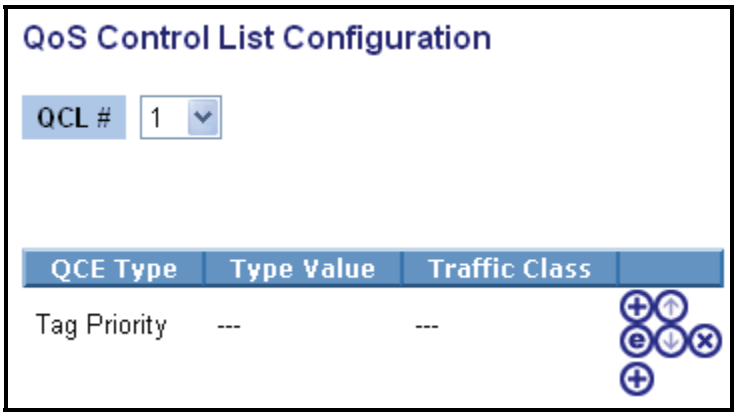


Fig. 3-62 Set up VLAN Tag Priority Mapping Finish

3-7. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to respond to the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

Parameters description:

SNMP:

The term SNMP here is used for the activation or de-activation of SNMP. Default is Enable.

Get/Set/Trap Community:

Community name is used as password for authenticating if the

requesting network management unit belongs to the same community group. If they both don’t have the same community name, they don’t belong to the same group. Hence, the requesting network management unit can not access the device with a different community name via SNMP protocol. If they both have the same community name, they can talk to each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. Blank spaces are not allowed in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can’t be applied to other functions such as SET and Trap.

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Enable

Default trap host IP address: 0.0.0.0

Default port number :162

Trap:

In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address and are user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from being lost.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponding trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. The Enterprise (no. 6) trap is classified as a private trap, which are listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

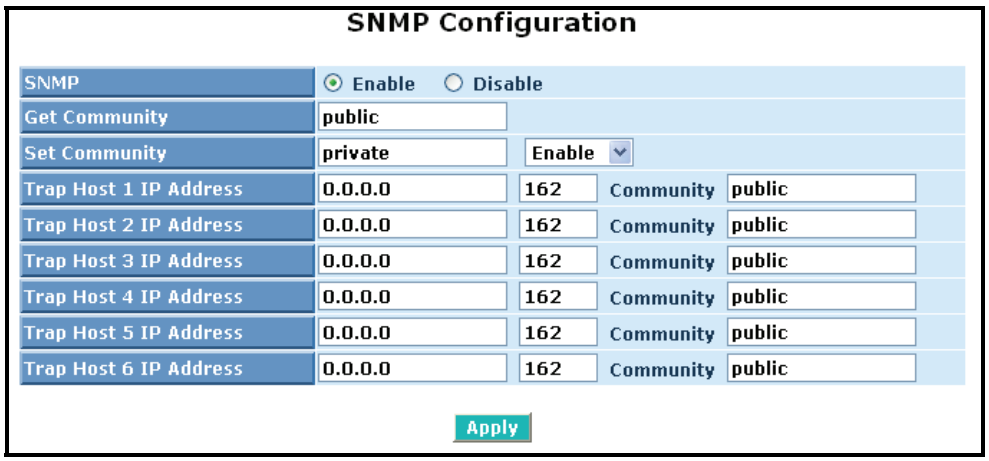


Fig. 3-63 Community and trap host setting

3-8. ACL

The SG71660MA switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way.

The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3-8-1.Ports

Function name:

ACL Port Configuration

Function description:

The switch ACL function supports up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies and each port can select one policy, then decides which of the following actions would be taken according to the packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters:

- Packet Deny or Permit
- Rate Limiter (Unit: pps)
- Port Copy (1 – 16)

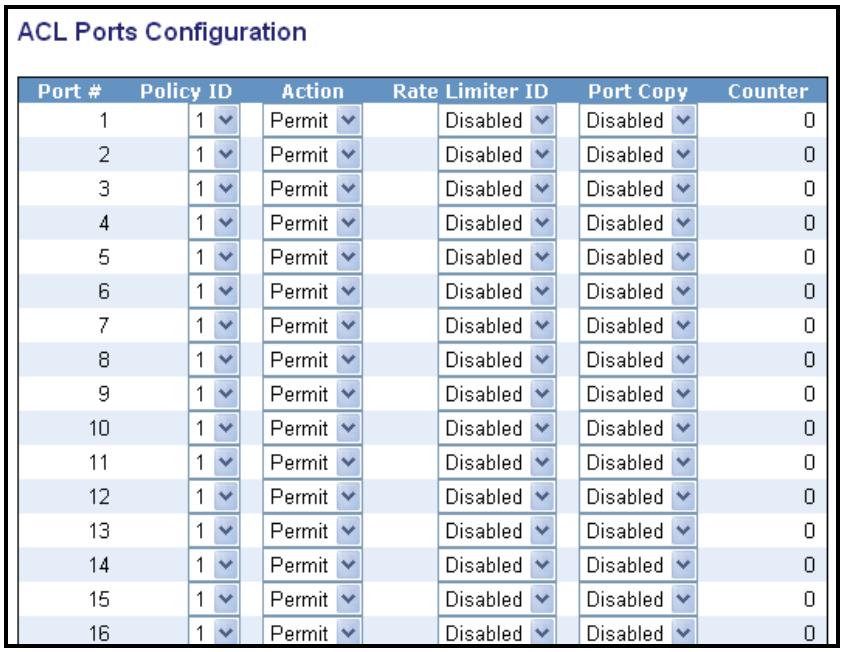

ACL Ports Configuration
Port # Policy ID Action Rate Limiter ID Port Copy Counter
1 1 Permit Disabled Disabled 0
2 1 Permit Disabled Disabled 0
3 1 Permit Disabled Disabled 0
4 1 Permit Disabled Disabled 0
5 1 Permit Disabled Disabled 0
6 1 Permit Disabled Disabled 0
7 1 Permit Disabled Disabled 0
8 1 Permit Disabled Disabled 0
9 1 Permit Disabled Disabled 0
10 1 Permit Disabled Disabled 0
11 1 Permit Disabled Disabled 0
12 1 Permit Disabled Disabled 0
13 1 Permit Disabled Disabled 0
14 1 Permit Disabled Disabled 0
15 1 Permit Disabled Disabled 0
16 1 Permit Disabled Disabled 0

Fig. 3-64

Parameter description:

Port #:

Port number: 1~16

Policy ID:

Policy ID range:1~8

Action:

Permit or Deny forwarding the ACL packets

Rate Limiter ID:

Disabled: Disable Rate Limitation

Rate Limiter ID Range: 1~16. To select one of rate limiter ID for this port, it will limit met ACL packets by rate limiter ID configuration.

Port Copy:

Disabled: Disable to copy the ACL packets to specific port

Port number: 1~16. Copy the ACL packets to the selected port

Counter: The counter will increase from initial value 0 when this port receives one of the ACL packets. The counter value will increase +1

3-8-2.Rate Limiters

Function name:

ACL Rate Limiter Configuration

Function description:

There are 16 rate limiter ID. You can assign one of the limiter ID for each port. The rate limit configuration unit is Packet Per Second (pps).

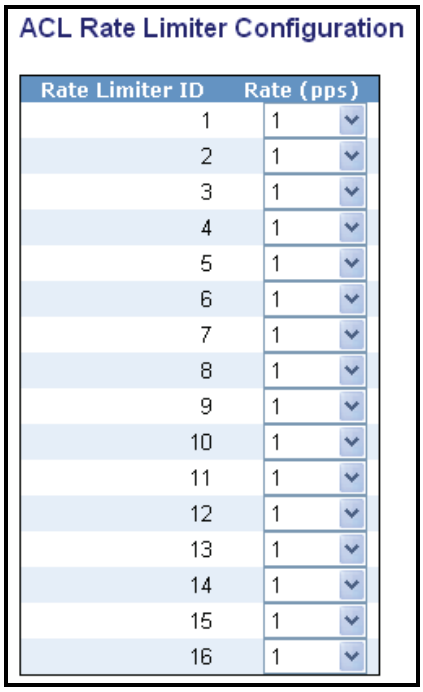


Fig. 3

Parameter description:

Rate Limiter ID:

ID Range: 1~16

Rate(pps):

1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

3-8-3.Access Control List

Function name:

ACL Rate Limiter Configuration

Function description:

The switch ACL function supports up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies and each port can select one policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would be taken according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

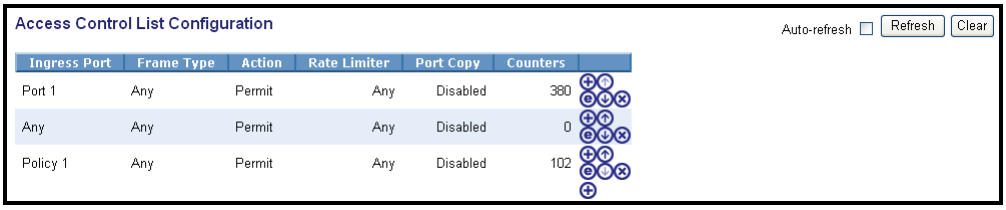
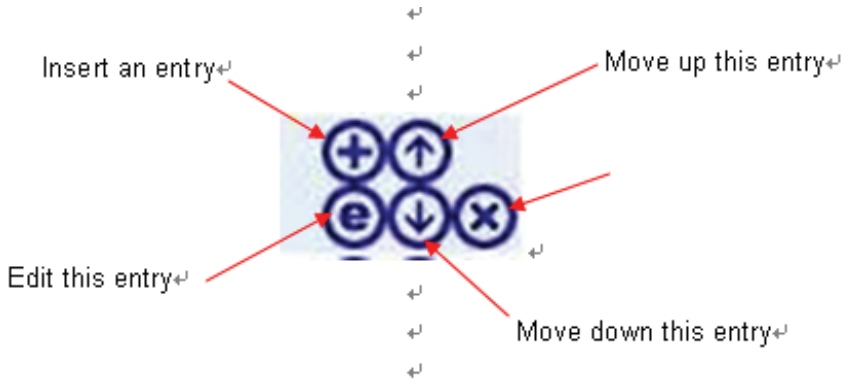


Fig. 3-66 Ingress Port



Parameter description:

Ingress Port:

Configurable Range: Any / Policy 1-8 / Port 1-16
Any: Apply this ACE rule for each port ingress classification
Policy 1-8: Apply this ACE rule for specific policy
Port 1-16: Apply this ACE rule for specific port ingress classification

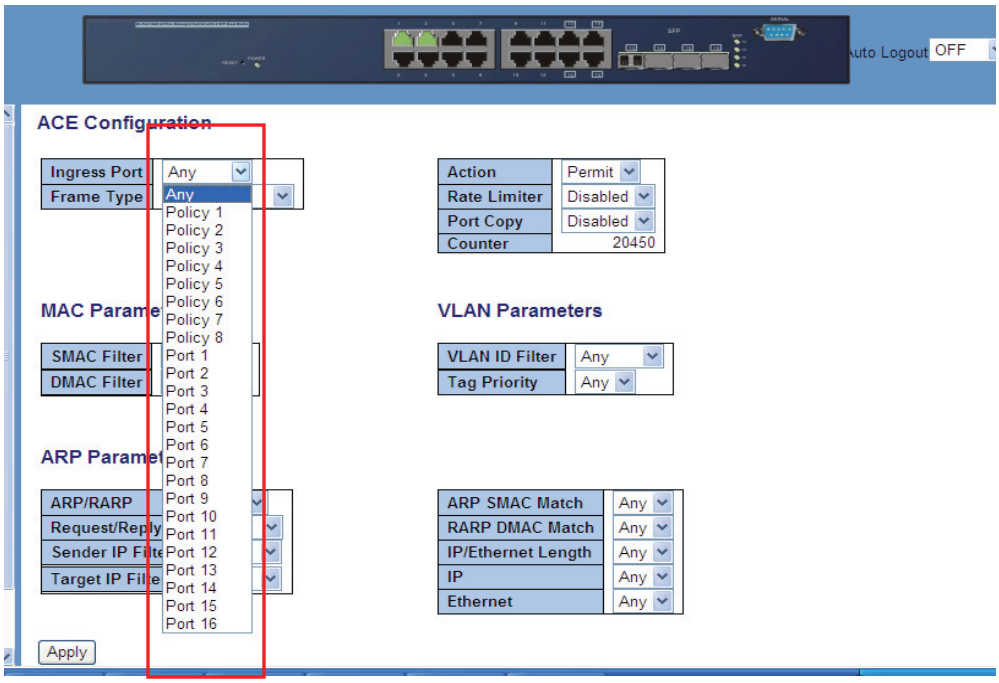


Fig. 3-67 Ingress Port

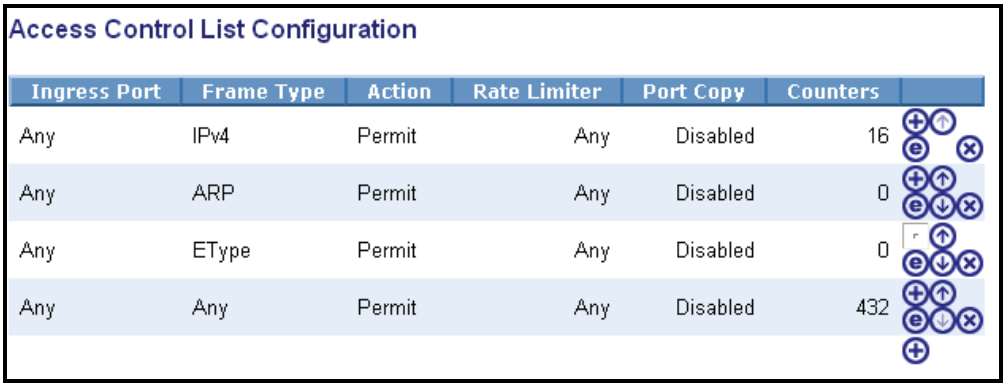


Fig. 3-68

Parameter description:

Frame Type:

Range: Any / Ethernet Type / ARP / IPv4
Any: It is including all frame types
Ethernet Type: It is including all Ethernet frame types
ARP: It is including all ARP protocol frame types
IPv4: It is including all IPv4 protocol frame types

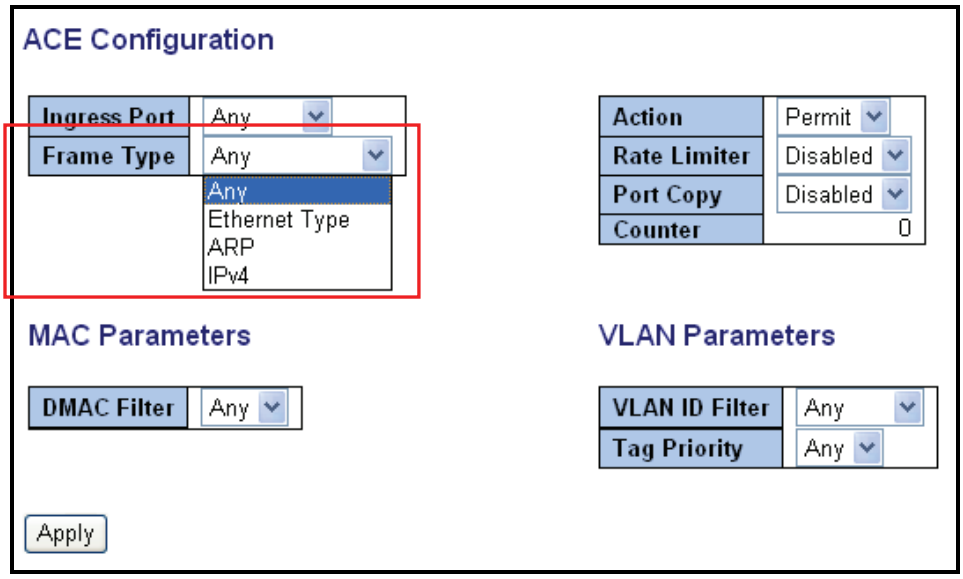


Fig. 3-69 Frame Type

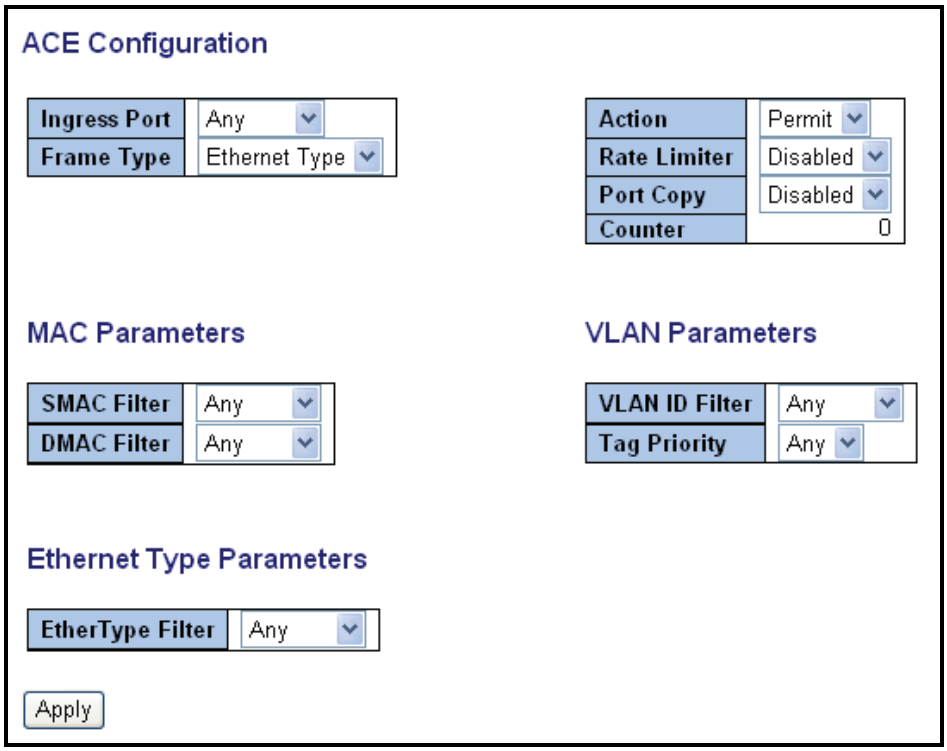


Fig. 3-70

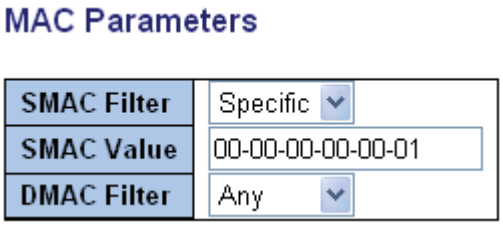


Fig. 3-71

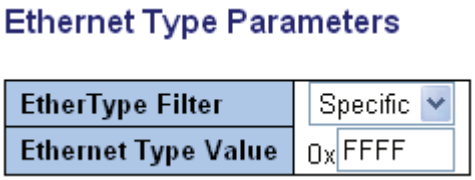


Fig. 3-72

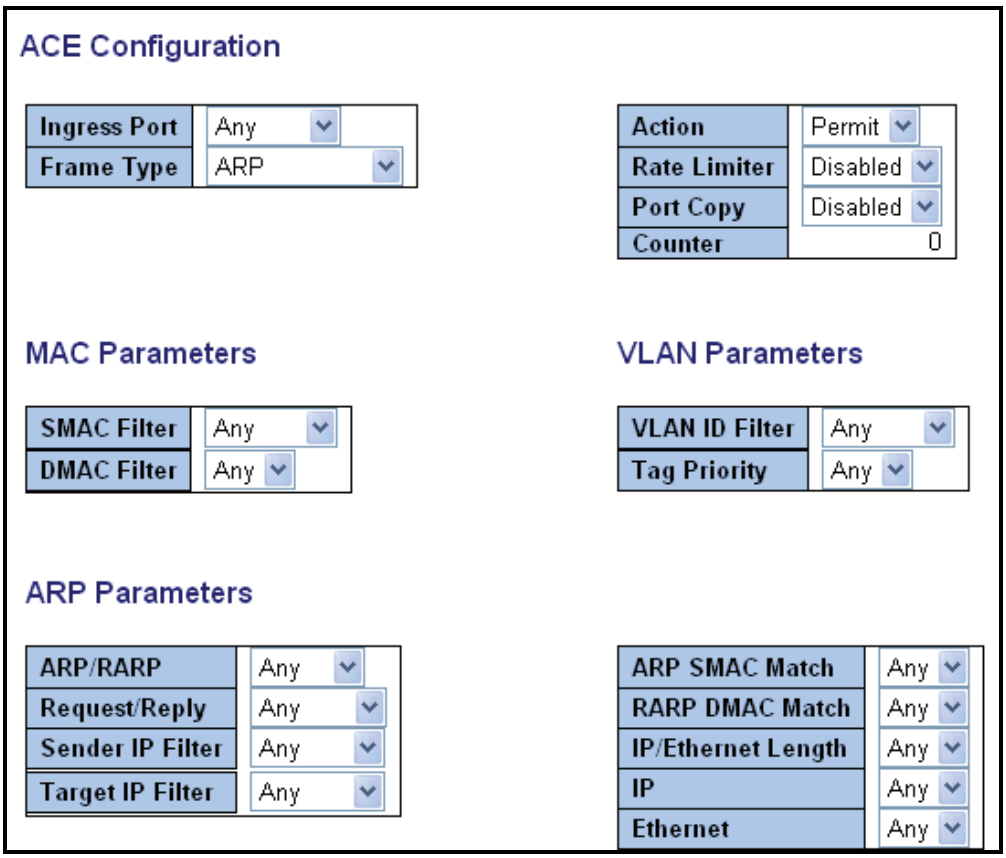


Fig. 3-73 ARP

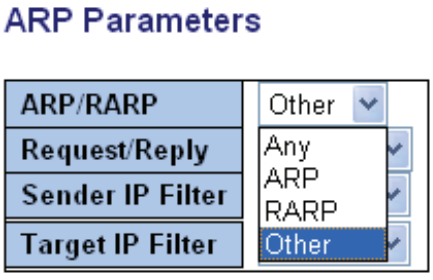


Fig. 3-74 ARP

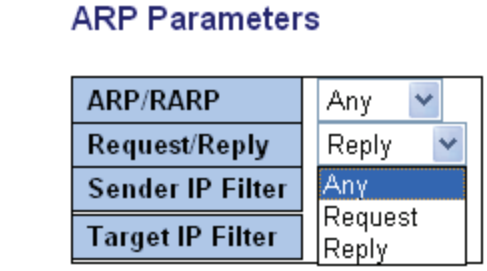


Fig. 3-75 ARP

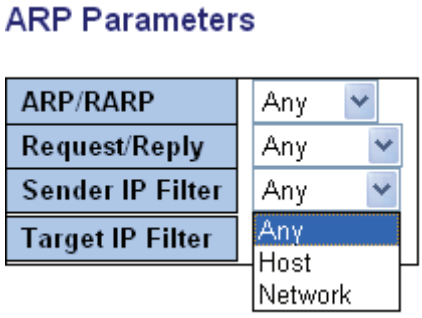


Fig. 3-76 ARP

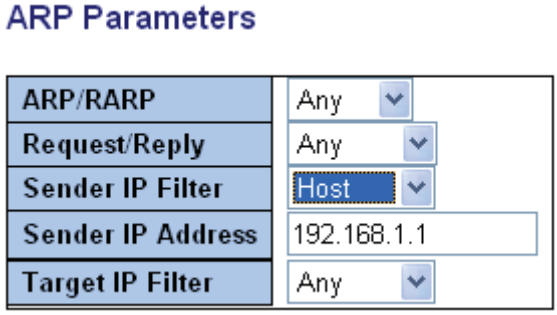


Fig. 3-77 ARP

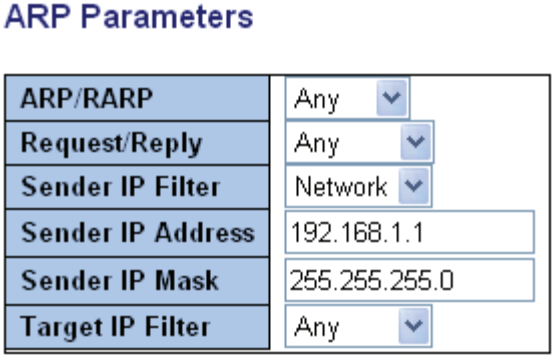


Fig. 3-78 ARP

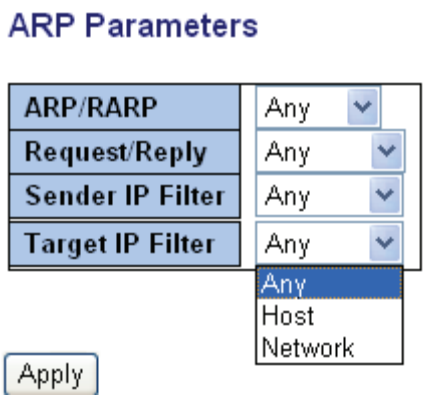


Fig. 3-79 ARP

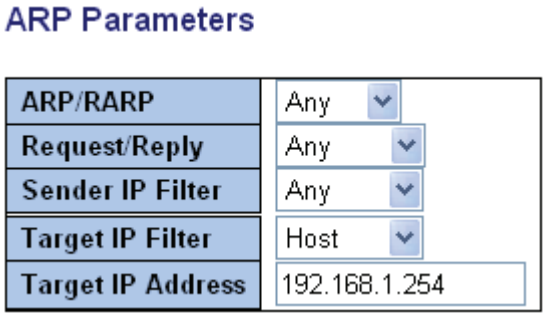


Fig. 3-80 ARP

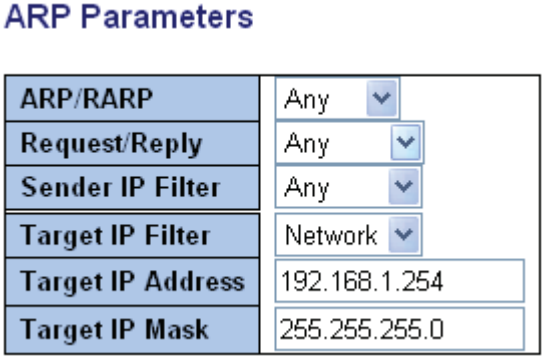


Fig. 3-81 ARP

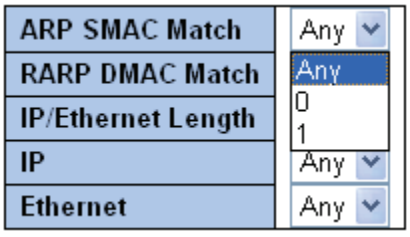


Fig. 3-83 ARP

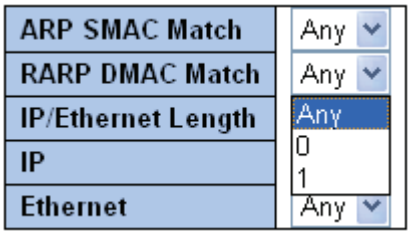


Fig. 3-84 ARP

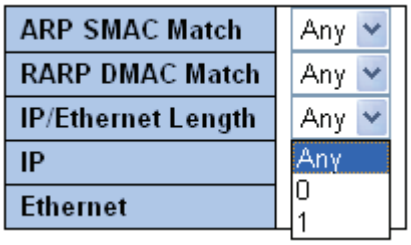


Fig. 3-85 ARP

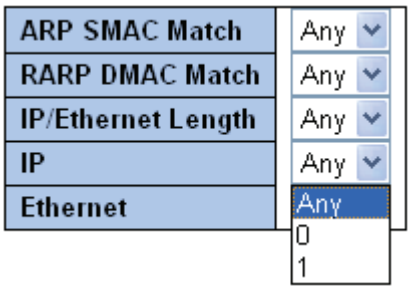


Fig. 3-86 ARP

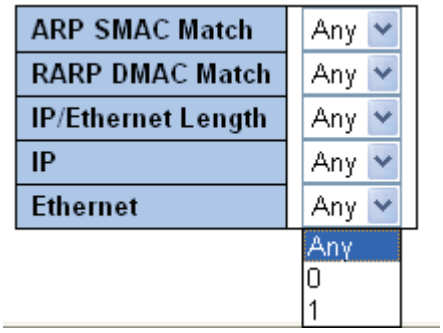


Fig. 3-87 ARP

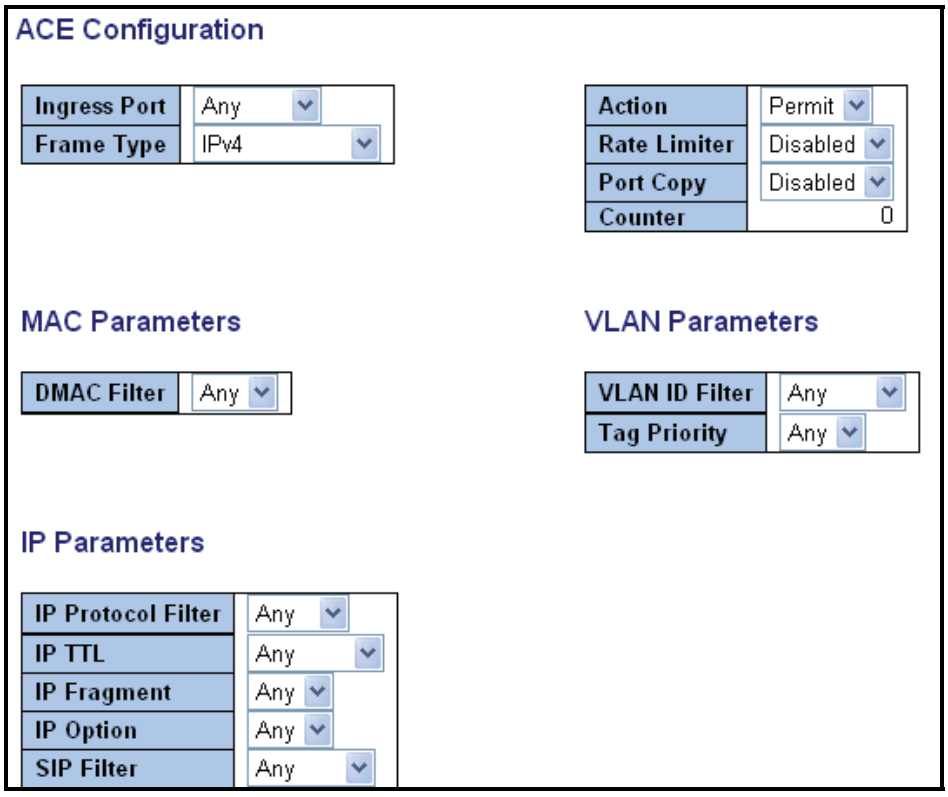


Fig. 3-88 IPv4

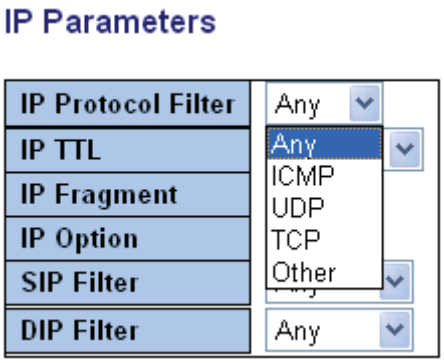


Fig. 3-89 IPv4

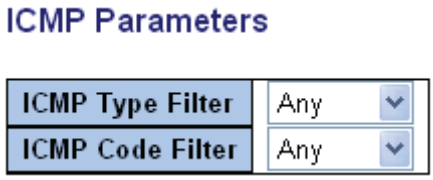


Fig. 3-90 IPv4

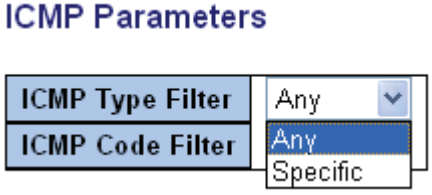


Fig. 3-91 IPv4

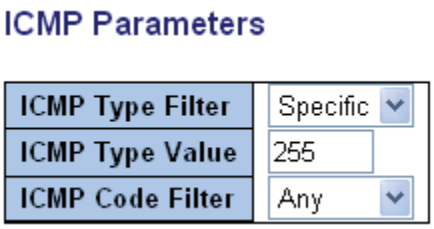


Fig. 3-92 IPv4

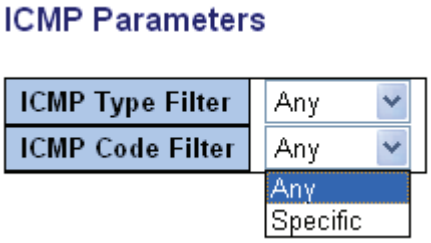


Fig. 3-93 IPv4

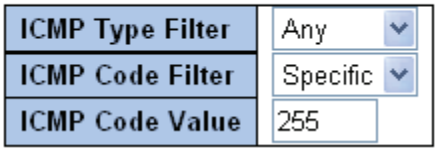


Fig. 3-94 IPv4

Fig. 3-95 IPv4

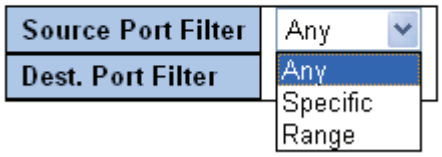


Fig. 3-96 IPv4

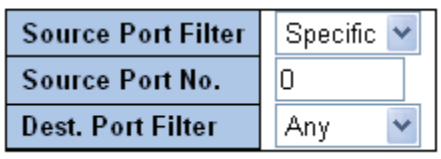


Fig. 3-97 IPv4

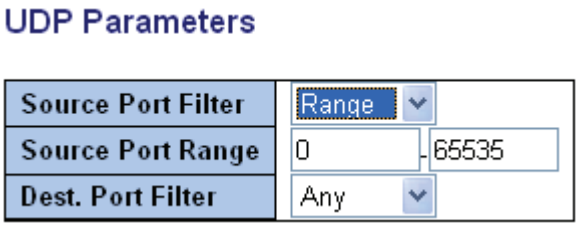


Fig. 3-98 IPv4

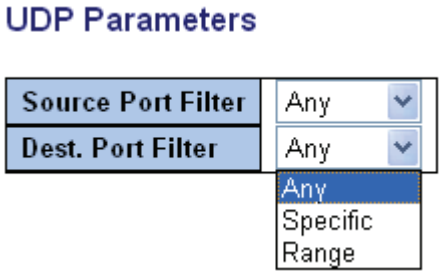


Fig. 3-99 IPv4

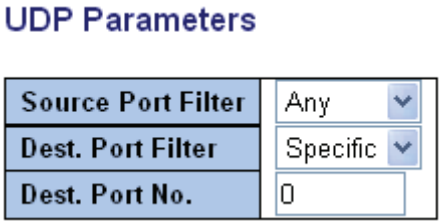


Fig. 3-100 IPv4

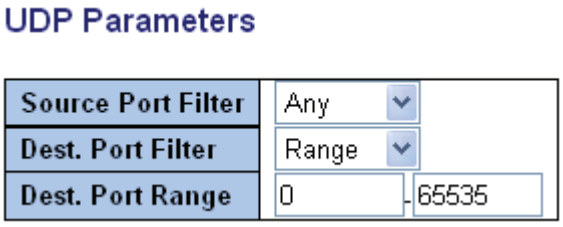


Fig. 3-101 IPv4

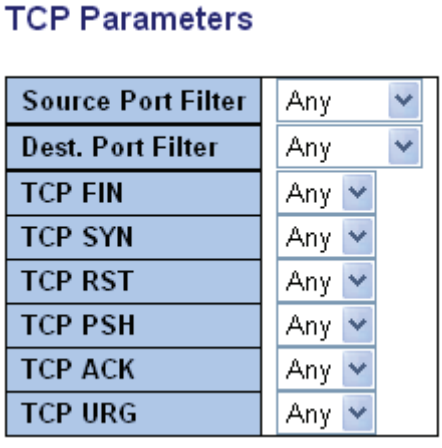


Fig. 3-102 IPv4

TCP Parameters

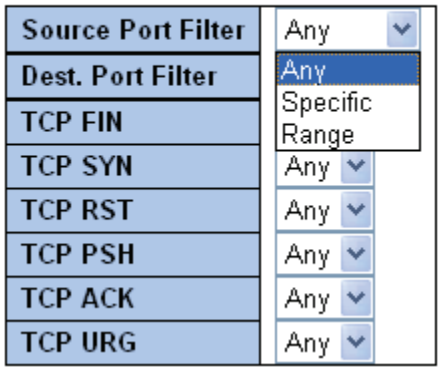


Fig. 3-103 IPv4

TCP Parameters

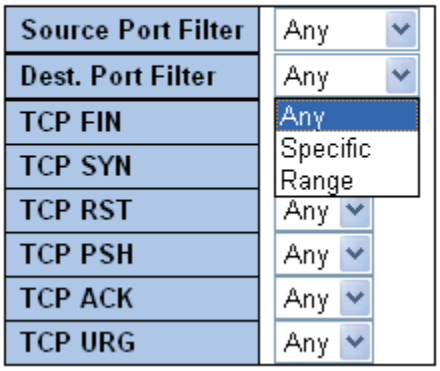


Fig. 3-104 IPv4

TCP Parameters

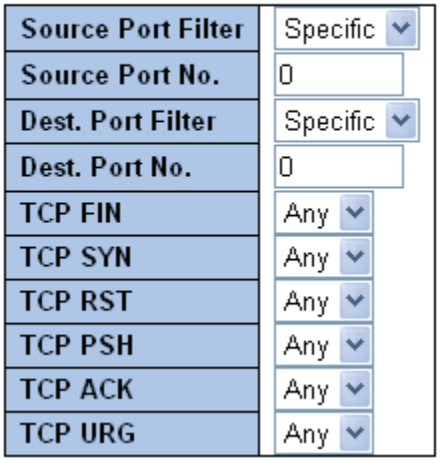


Fig. 3-105 IPv4

TCP Parameters

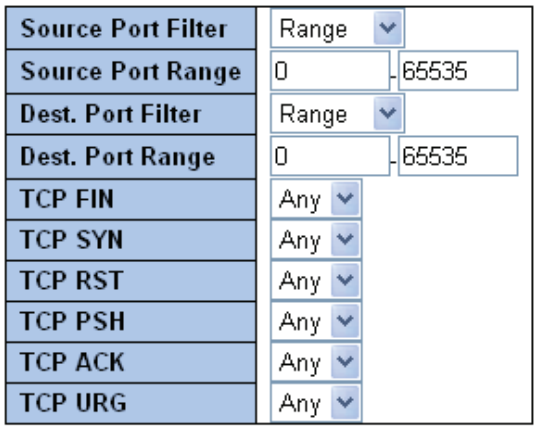


Fig. 3-106 IPv4

TCP Parameters

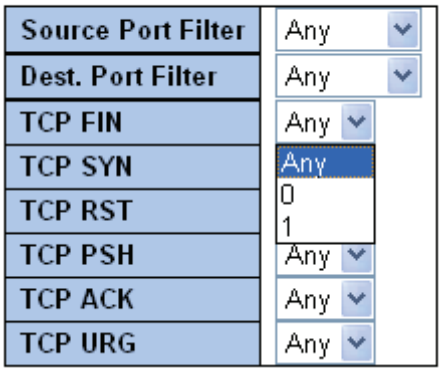


Fig. 3-107 IPv4

IP Parameters

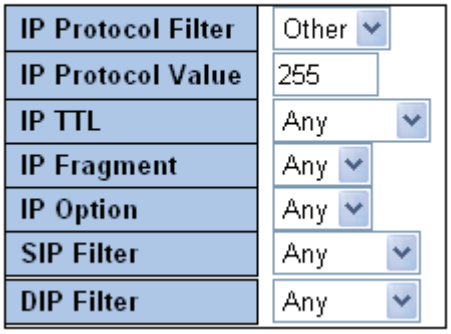


Fig. 3-108 IPv4

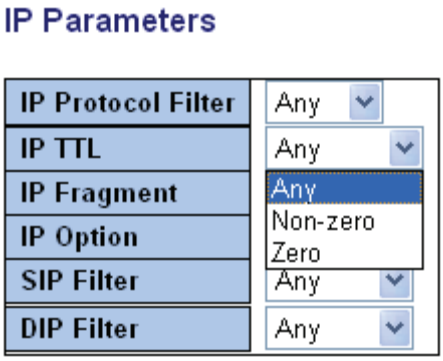


Fig. 3-109 IPv4

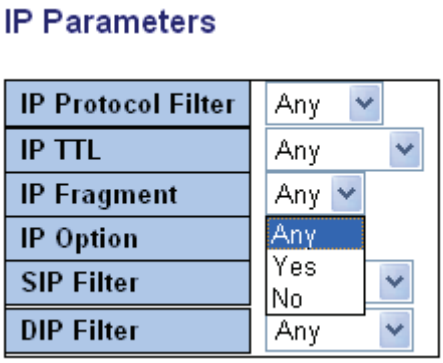


Fig. 3-110 IPv4

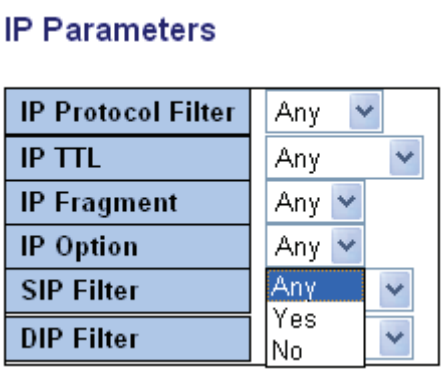


Fig. 3-111 IPv4

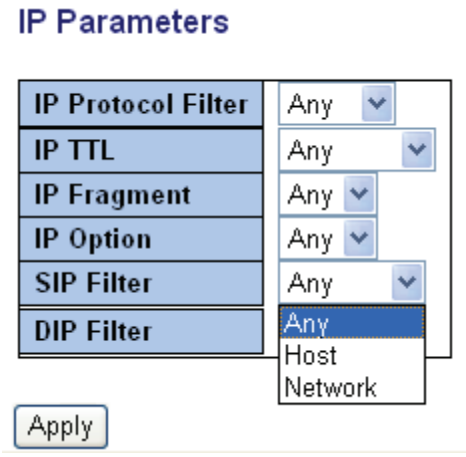


Fig. 3-112 IPv4

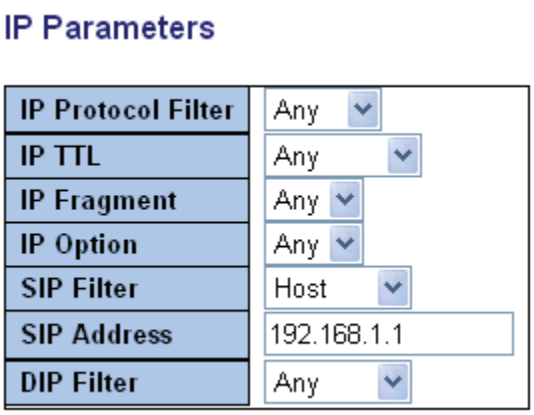


Fig. 3-113 IPv4

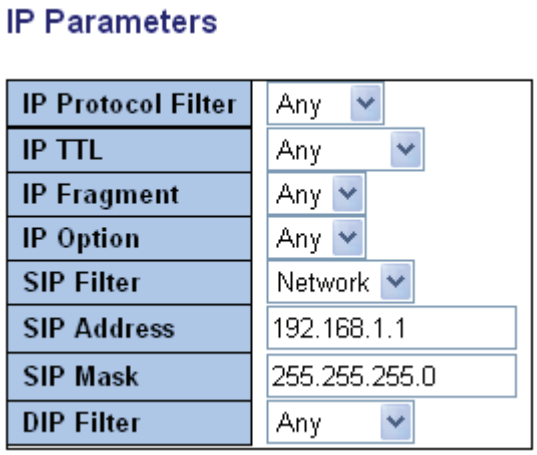


Fig. 3-114 IPv4

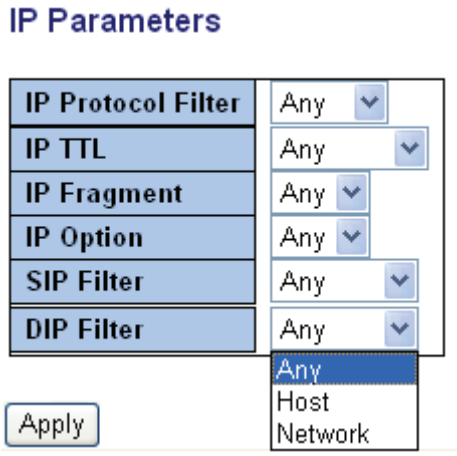


Fig. 3-115 IPv4

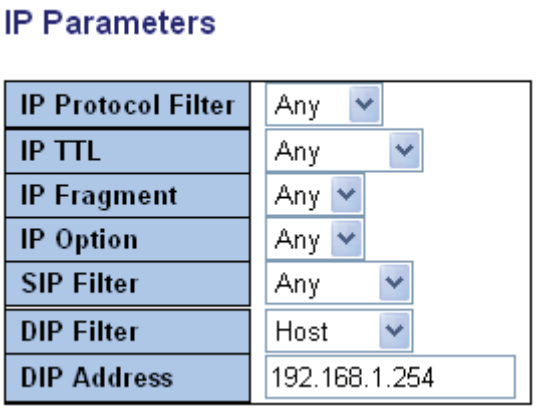


Fig. 3-116 IPv4

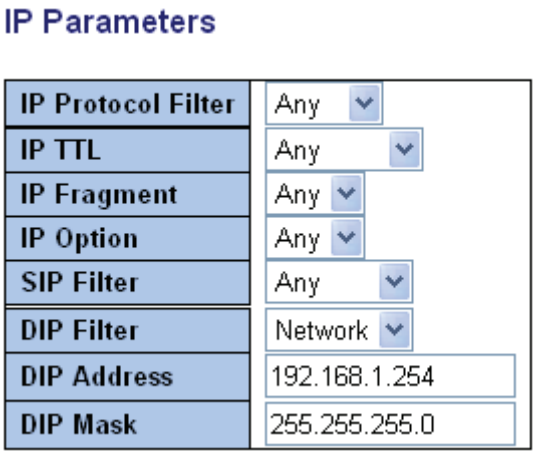


Fig. 3-117 IPv4

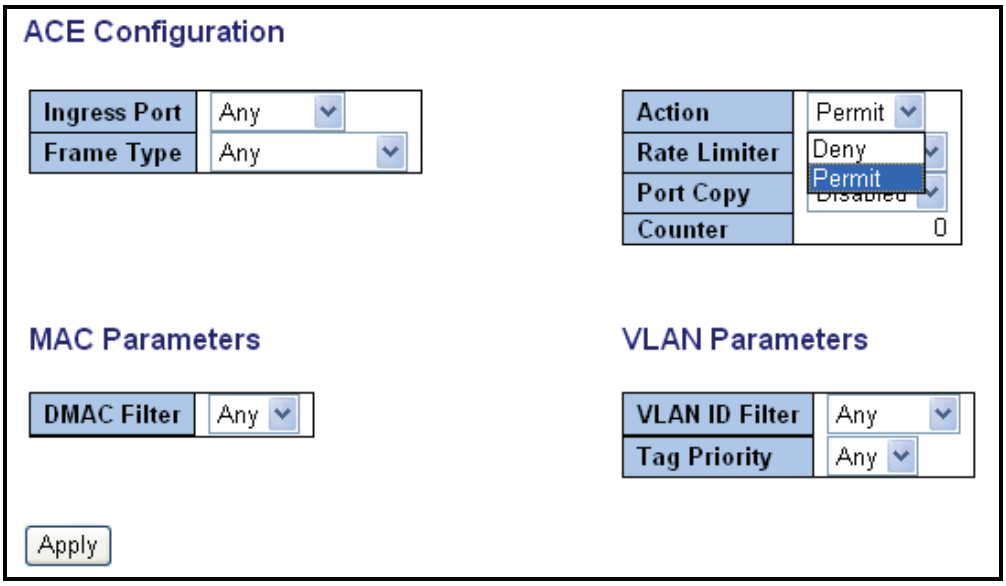


Fig. 3-118 Action

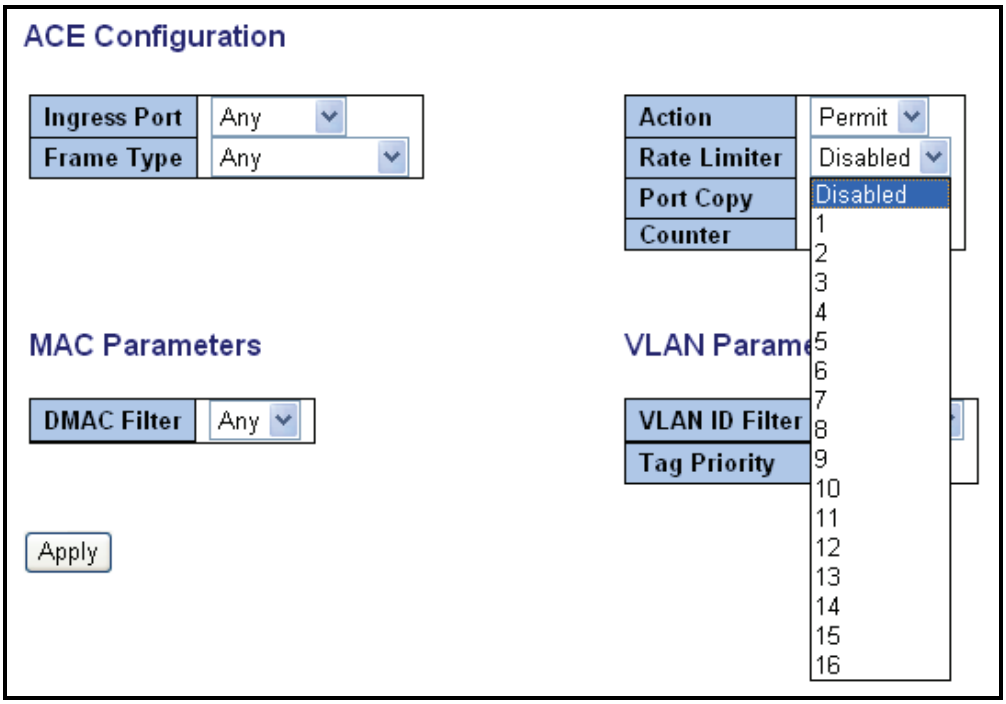


Fig. 3-119 Rate Limiter

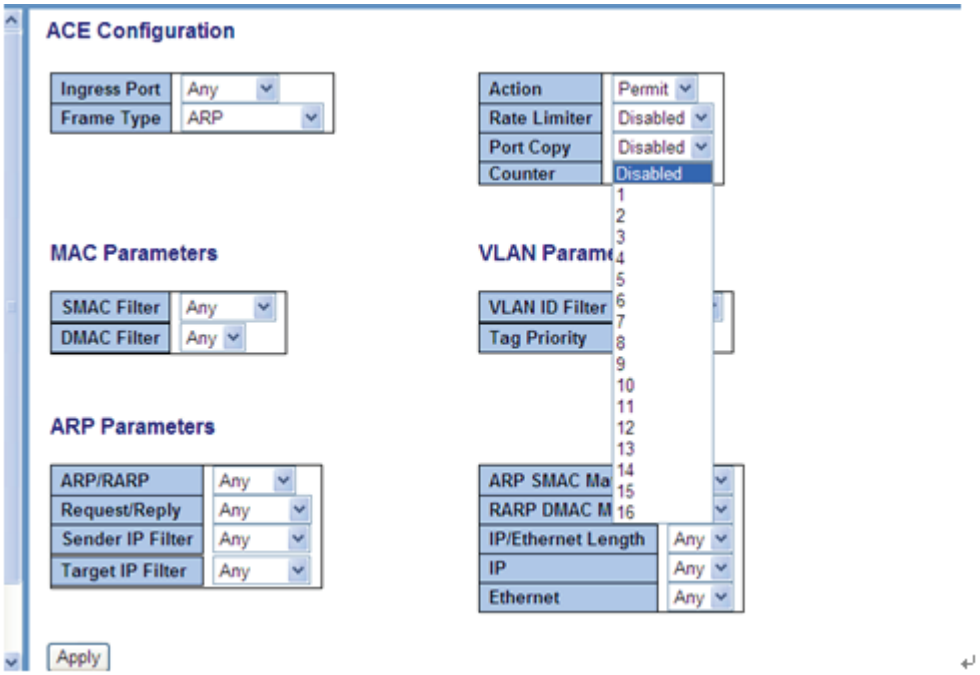


Fig. 3-120 Port Copy

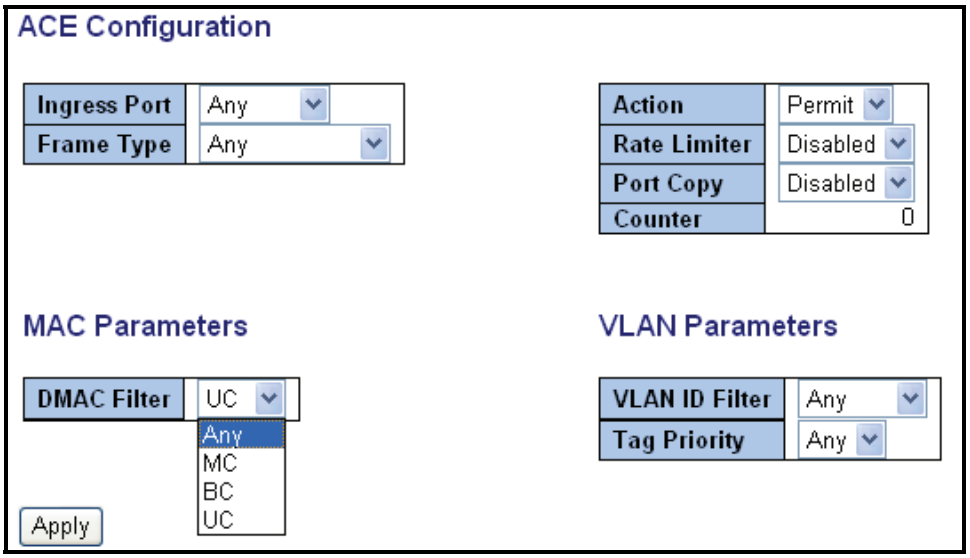


Fig. 3-121 DMAC Filter

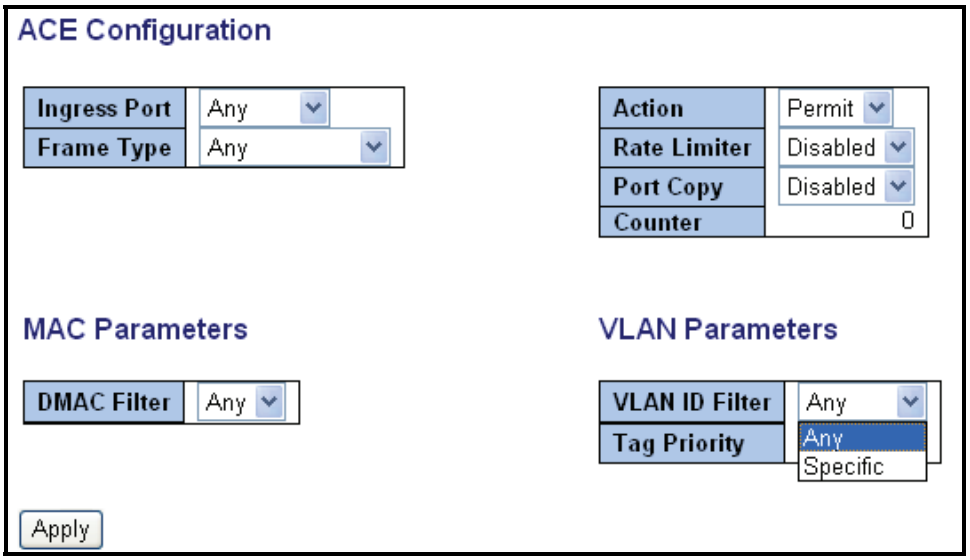


Fig. 3-122 VLAN ID Filter

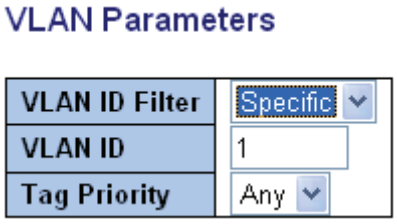


Fig. 3-123 VLAN ID Filter

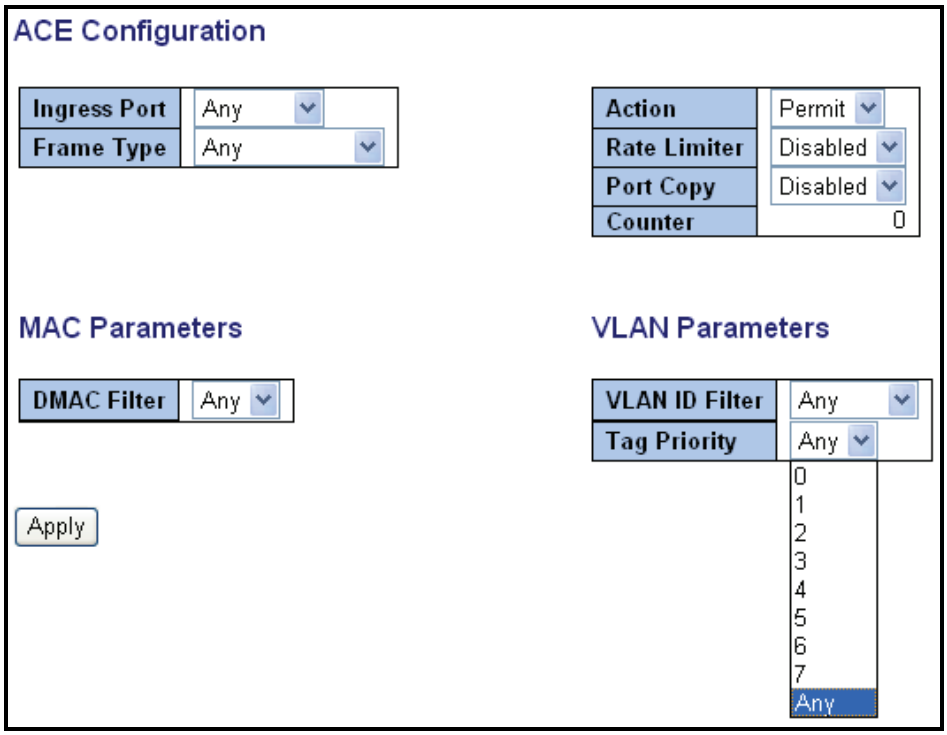


Fig. 3-124 Tag Priority

Function name:

ACE Configuration

Function description:

The switch ACL function supports up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies and each port can select one policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would be taken according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

Parameter description:

Ingress Port:

Range: Any / Policy 1-8 / Port 1-16
Any: Apply this ACE rule for each port ingress classification
Policy 1-8: Apply this ACE rule for specific policy
Port 1-16: Apply this ACE rule for specific port ingress classification

IP Protocol Filter:

Range: Any / Ethernet Type / ARP / IPv4
Any: It is including all frame types
Ethernet Type: It is including all Ethernet frame types
ARP: It is including all ARP protocol frame types
IPv4: It is including all IPv4 protocol frame types

MAC Parameters: (When Frame Type = Any)

DMAC Filter:

Range: Any / MC / BC / UC

Any: It is including all destination MAC addresses
MC: It is including all Multicast MAC addresses
BC: It is including all Broadcast MAC addresses
UC: It is including all Unicast MAC addresses

MAC Parameters: (When Frame Type = Ethernet Type)

SMAC Filter:

Range: Any / Specific

Any: It is including all source MAC addresses
Specific: It is according to SMAC Value specific the source MAC address

DMAC Filter:

Range: Any / MC / BC / UC / Specific

Any: It is including all destination MAC addresses
MC: It is including all Multicast MAC addresses
BC: It is including all Broadcast MAC addresses
UC: It is including all Unicast MAC addresses
Specific: It is according to DMAC Value specific the destination MAC address

MAC Parameters: (When Frame Type = ARP)

SMAC Filter:

Range: Any / Specific

Any: It is including all source MAC address
Specific: It is according to SMAC Value specific the source MAC address

DMAC Filter:

Range: Any / MC / BC / UC

Any: It is including all destination MAC addresses
MC: It is including all Multicast MAC addresses
BC: It is including all Broadcast MAC addresses
UC: It is including all Unicast MAC addresses

MAC Parameters: (When Frame Type = IPv4)

DMAC Filter:

Range: Any / MC / BC / UC

Any: It is including all destination MAC addresses
MC: It is including all Multicast MAC addresses
BC: It is including all Broadcast MAC addresses
UC: It is including all Unicast MAC addresses

Ether Type Parameters: (When Frame Type = Ethernet Type)

EtherType Filter:

Range: Any / Specific

Any: It is including all Ethernet frame type
Specific: It is according to specific Ethernet Type Value.

Ethernet Type Value:

The Ethernet Type Range: 0x600-0xFFFF

ARP Parameters: (When Frame Type = ARP)

ARP/RARP:
Range: Any / ARP / RARP / Other
Any: Including all ARP/RARP protocol frame types
ARP: Including all ARP protocol frame types
RARP: Including all RARP frame types
Other: Including other frame types except ARP/RARP protocol

Request/Reply:

Range: Any / Request / Reply
Any: Including all ARP/RARP Request and Reply
Request: Including all ARP/RARP request frames
Reply: Including all ARP/RARP reply frames

Sender IP Filter:
Range: Any / Host / Network
Any: Including all sender IP address
Host: Only one specific sender host IP address
Network: A specific IP subnet segment under the sender IP mask

Sender IP Address:
Default: 192.168.1.1

Sender IP Mask:
Default: 255.255.255.0

Target IP Filter:
Range: Any / Host / Network
Any: Including all target IP address
Host: Only one specific target host IP address
Network: A specific IP subnet segment under the target IP mask

Target IP Address:
Default: 192.168.1.254

Target IP Mask:
Default: 255.255.255.0

ARP SMAC Match:
Range: Any / 0 / 1
Any:
Both 0 and 1
0:
The ingress ARP frames where the source MAC address is not equal to SMAC under MAC parameter setting
1:
The ingress ARP frames where the source MAC address is equal to SMAC address under MAC parameter setting

RARP DMAC Match:
Range: Any / 0 / 1
Any:
Both 0 and 1
0:
The ingress RARP frames where the Destination MAC address is not equal to DMAC address under MAC parameter setting
1:
The ingress RARP frames where the Destination MAC address is equal to DMAC address under MAC parameter setting

IP/Ethernet Length:
Range: Any / 0 / 1
Any:
Both 0 and 1
0:
The ingress ARP/PARP frames where the Hardware size is not equal to "0x6" or the Protocol size is not equal "0x4"
1:

The ingress ARP/PARP frames where the Hardware size is equal to "0x6" and the Protocol size is "0x4"

IP:

Range: Any / 0 / 1

Any:

Both 0 and 1

0:

The ingress ARP/PARP frames where Protocol type is not equal to "0x800"

1:

The ingress ARP/PARP frames where Protocol type is equal to "0x800"

Ethernet:

Range: Any / 0 / 1

Any:

Both 0 and 1

0:

The ingress ARP/PARP frames where Hardware type is not equal to "0x100"

1:

The ingress ARP/PARP frames where Hardware type is equal to "0x100"

IP Parameters: (When Frame Type = IPv4 and IP Protocol Filter = Any)

IPTTL: (Time To Live)

How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever

Range: Any / Non-zero / Zero

Any: Including all conditions for IPTTL

Non-Zero: Including IPTTL is Non-Zero

Zero: Including IPTTL is zero

IP Fragment: (IP Fragmentation Flag)

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.

Range: Any / Yes / No

Any: Including all IP fragment case

Yes: The ingress frame is fragmented packet

No: The ingress frames is not fragmented packet

IP Option:

A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Range: Any / Yes / No

Any: Including all IP option case
Yes: The ingress frame is specified IP options
No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Including all source IP address
Host: Only one specific source host IP address

Network: A specific IP subnet segment under the source IP mask

SIP Address:

Default: 192.168.1.1

SIP Mask:

Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Including all destination IP address
Host: Only one specific destination host IP address
Network: A specific IP subnet segment under the destination IP mask

DIP Address:

Default: 192.168.1.254

DIP Mask:

Default: 255.255.255.0

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = ICMP)

ICMP Type Filter:

Range: Any / Specific

Any: Including all types of ICMP type values

Specific: According to following ICMP type value setting for ingress classification

ICMP Type Value:

Range: 0-255

ICMP Code Filter:

Range: Any / Specific

Any: Including all of ICMP code values

Specific: According to following ICMP code value setting for ingress classification

ICMP Code Value:

Range: 0-255

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = UDP)

Source Port Filter:

Range: Any / Specific / Range

Any: Including all UDP source ports
Specific:
According to following Source Port No. setting for ingress classification
Range:
According to following Source Port Range setting for ingress classification

Source Port No.:

Range: 0-65535

Source Port Range.:

Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Including all UDP destination ports
Specific:

According to following Dest. Port No. setting for ingress classification

Range:

According to following Dest. Port Range setting for ingress classification

Dest. Port No.: (Destination Port Number)

Range: 0-65535

Dest. Port Range.: (Destination Port Range)

Range: 0-65535

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = TCP)

Source Port Filter:

Range: Any / Specific / Range

Any: Including all TCP source ports

Specific:

According to following Source Port No. setting for ingress classification

Range:

According to following Source Port Range setting for ingress classification

Source Port No.:

Range: 0-65535

Source Port Range.:

Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Including all TCP destination ports

Specific:

According to following Dest. Port No. setting for ingress classification

Range:

According to following Dest. Port Range setting for ingress classification

Dest. Port No.:

Range: 0-65535

Dest. Port Range.:

Range: 0-65535

TCP FIN:

TCP Control Bit FIN: Means No more data from sender

Range: Any / 0 / 1

Any: Including all TCP FIN case

0: The TCP control bit FIN is 0

1: The TCP control bit FIN is 1

TCP SYN:

TCP Control Bit SYN: Means Synchronize sequence numbers

Range: Any / 0 / 1

Any: Including all TCP SYN case

0: The TCP control bit SYN is 0

1: The TCP control bit SYN is 1

TCP RST:

TCP Control Bit RST: Means Reset the connection

Range: Any / 0 / 1

Any: Including all TCP RST case

0: The TCP control bit RST is 0

1: The TCP control bit RST is 1

TCP PSH:

TCP Control Bit PSH: Means Push Function

Range: Any / 0 / 1

Any: Including all TCP PSH case

0: The TCP control bit PSH is 0

1: The TCP control bit PSH is 1

TCP ACK:

TCP Control Bit ACK: Means Acknowledgment field significant

Range: Any / 0 / 1

Any: Including all TCP ACK case

0: The TCP control bit ACK is 0

1: The TCP control bit ACK is 1

TCP URG:

TCP Control Bit URG: Means Urgent Pointer field significant

Range: Any / 0 / 1

Any: Including all TCP URG case

0: The TCP control bit URG is 0

1: The TCP control bit URG is 1

IP Protocol Value:

The IP Protocol Value TCP options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. Currently defined options include (kind indicated in octal):
0 - End of option list
1 - No-Operation

Range: Any / 0 / 1

Any: Including all IP protocol value case

0: The IP protocol value is 0

1: The IP protocol value is 1

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = Other)

IP Protocol Value

Default: 255

IPTTL: (Time To Live)

How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever

Range: Any / Non-zero / Zero

Any: Including all conditions for IPTTL

Non-Zero: Including IPTTL is Non-Zero

Zero: Including IPTTL is zero

IP Fragment: (IP Fragmentation Flag)

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.

Range: Any / Yes / No

Any: Including all IP fragment case

Yes: The ingress frame is fragmented packet

No: The ingress frames is not fragmented packet

IP Option:

A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Range: Any / Yes / No

Any: Including all IP option case
Yes: The ingress frame is specified IP options
No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Including all source IP address
Host: Only one specific source host IP address
Network: A specific IP subnet segment under the source IP mask

SIP Address:

Default: 192.168.1.1

SIP Mask:

Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Including all destination IP address
Host: Only one specific destination host IP address
Network: A specific IP subnet segment under the destination IP mask

DIP Address:

Default: 192.168.1.254

DIP Mask:

Default: 255.255.255.0

VLAN Parameters:

VLAN ID Filter:

Range: Any / Specific
Any: Including all VLAN IDs
Specific: According to following VLAN ID and Tag Priority setting for ingress classification

VLAN ID:

Range: 1-4094

Tag Priority:

Range: Any / 0-7

Any: Including all Tag Priority values
0-7: The Tag Priority Value is one of number (0-7)

Action Parameters:

When the ingress frame meets above ACL ingress classification rule you can do the following actions:

Action:

Range: Permit / Deny
Permit:
Permit the ACL ingress classification rule packets forwarding to other ports on the switch
Deny:
Discard the ACL ingress classification rule packets

Rate Limiter:

Range: Disabled / 1-16
Disable: Disable Rate Limiter function
1-16: Apply the Rate Limiter Number setting for met ACL ingress rule packets

Port Copy:

Range: Disabled / 1-16
Disable: Disable the Port Copy function
1-16: The packets will be copied to the selected port when they meet ACL ingress rule.

3-8-4.Wizard

Function name:

Wizard

Function description:

The wizard function provides 4 types of typical applications for the user to easily configure their application with ACL function.

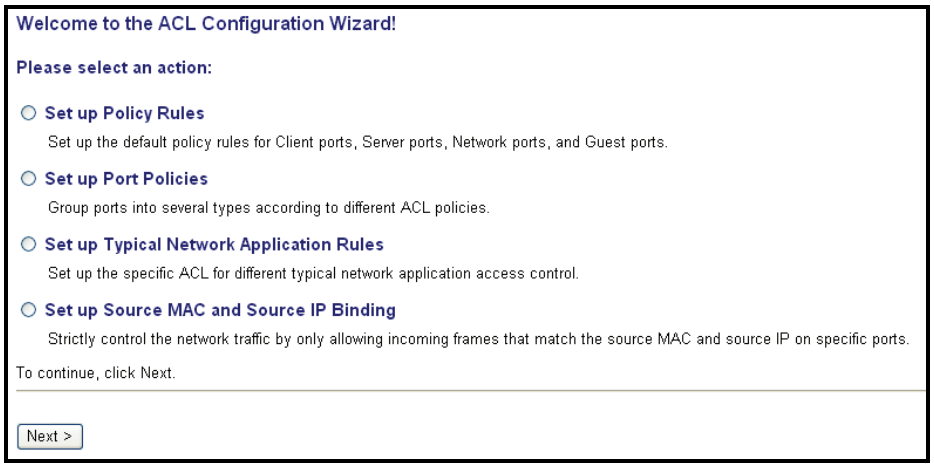

Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
To continue, click Next.
Next >

Fig. 3-125 Wizard

Parameter description:

Please select an Action:

Set up Policy Rules / Set up Port Policies / Set up Typical Network Application Rules / Set up Source MAC and Source IP Binding

Next:

Click on <Next> to confirm current setting and go to next step automatically.

Cancel:

Cancel current setting back to top layer in the ACL wizard function

Back:

Click on <Back> to back to previous step

Wizard Again:

Click on <Wizard Again> the UI will back to top layer in the wizard function

Finish:

Click on <Finish> to finish the ACL Wizard settings. It will, change the related parameters. Click on <Apply> to confirm the all changes.

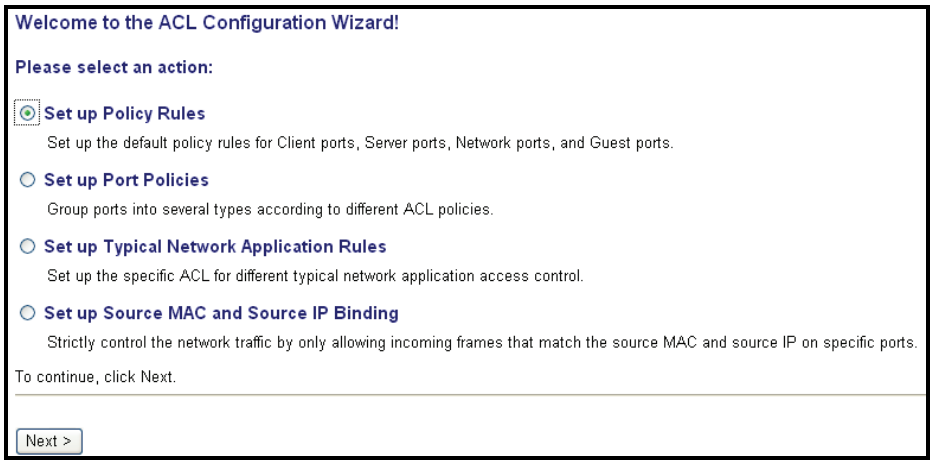

Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
To continue, click Next.
Next >

Fig. 3-126 Set up Policy Rules

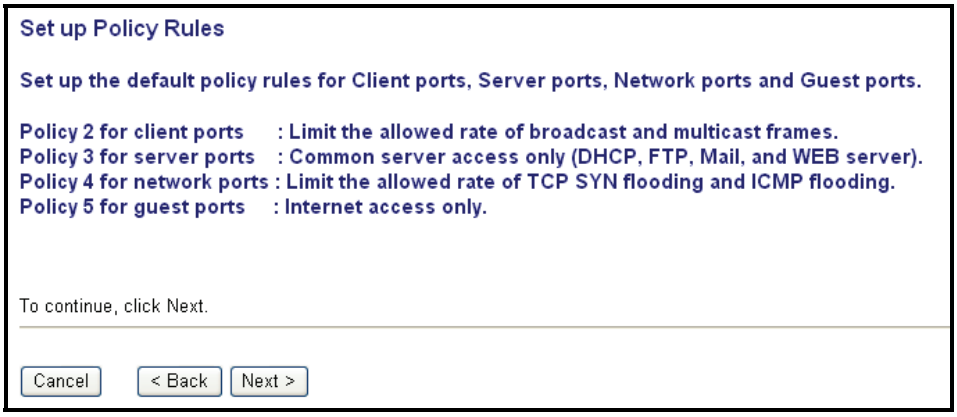

Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Policy 2 for client ports : Limit the allowed rate of broadcast and multicast frames.
Policy 3 for server ports : Common server access only (DHCP, FTP, Mail, and WEB server).
Policy 4 for network ports : Limit the allowed rate of TCP SYN flooding and ICMP flooding.
Policy 5 for guest ports : Internet access only.
To continue, click Next.
Cancel
< Back
Next >

Fig. 3-127 Set up Policy Rules

Finished !
The ACL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-128 Set up Policy Rules

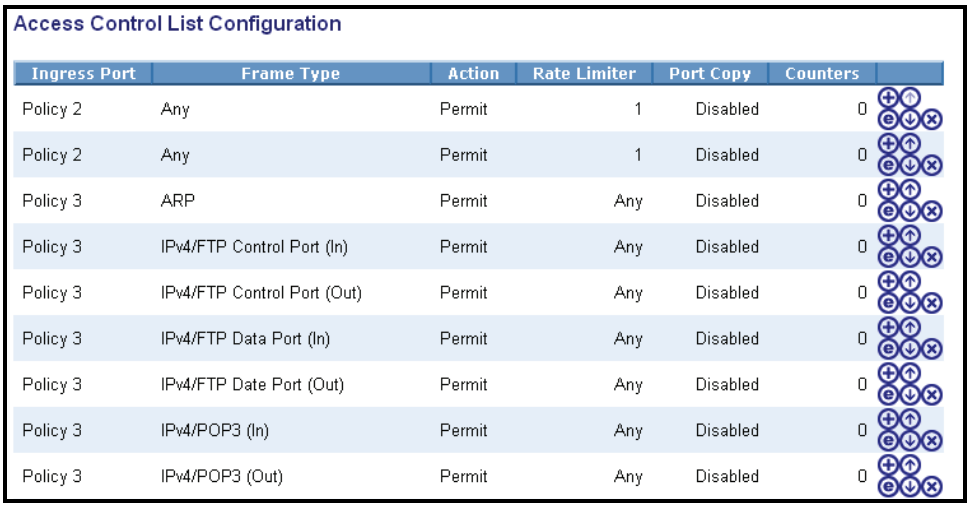

Access Control List Configuration
Ingress Port
Frame Type
Action
Rate Limiter
Port Copy
Counters
Policy 2 Any Permit 1 Disabled 0
Policy 2 Any Permit 1 Disabled 0
Policy 3 ARP Permit Any Disabled 0
Policy 3 IPv4/FTP Control Port (In) Permit Any Disabled 0
Policy 3 IPv4/FTP Control Port (Out) Permit Any Disabled 0
Policy 3 IPv4/FTP Data Port (In) Permit Any Disabled 0
Policy 3 IPv4/FTP Date Port (Out) Permit Any Disabled 0
Policy 3 IPv4/POP3 (In) Permit Any Disabled 0
Policy 3 IPv4/POP3 (Out) Permit Any Disabled 0

Fig. 3-129 Set up Policy Rules Finish

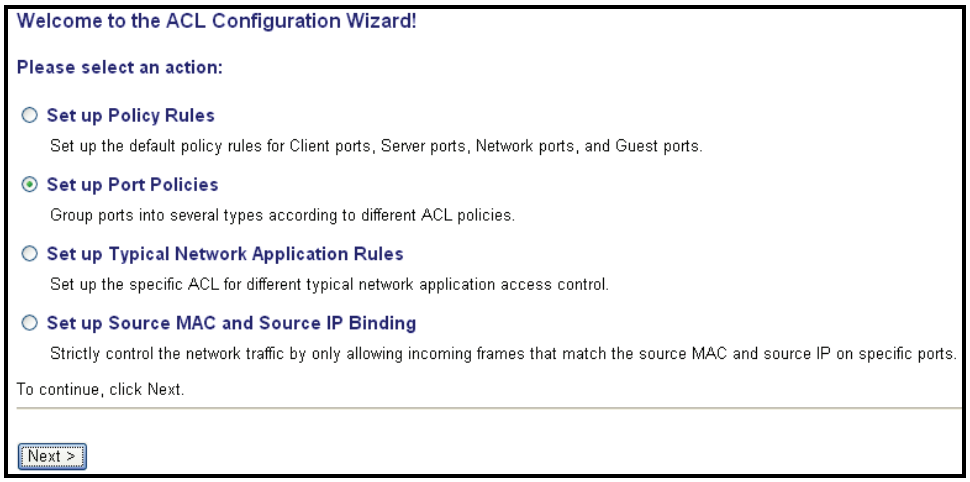

Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
To continue, click Next.
Next >

Fig. 3-130 Set up Port Policies

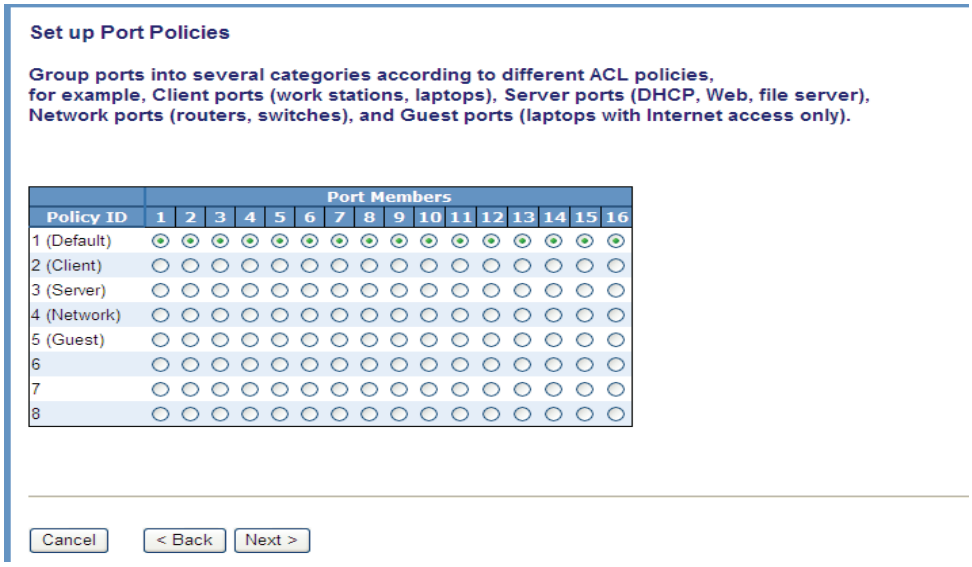

Set up Port Policies
Group ports into several categories according to different ACL policies,
for example, Client ports (work stations, laptops), Server ports (DHCP, Web, file server),
Network ports (routers, switches), and Guest ports (laptops with Internet access only).
Port Members
Policy ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
1 (Default)
2 (Client)
3 (Server)
4 (Network)
5 (Guest)
6
7
8
Cancel
< Back
Next >

Fig. 3-131 Set up Port Policies

Finished !
The ACL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-132 Set up Port Policies

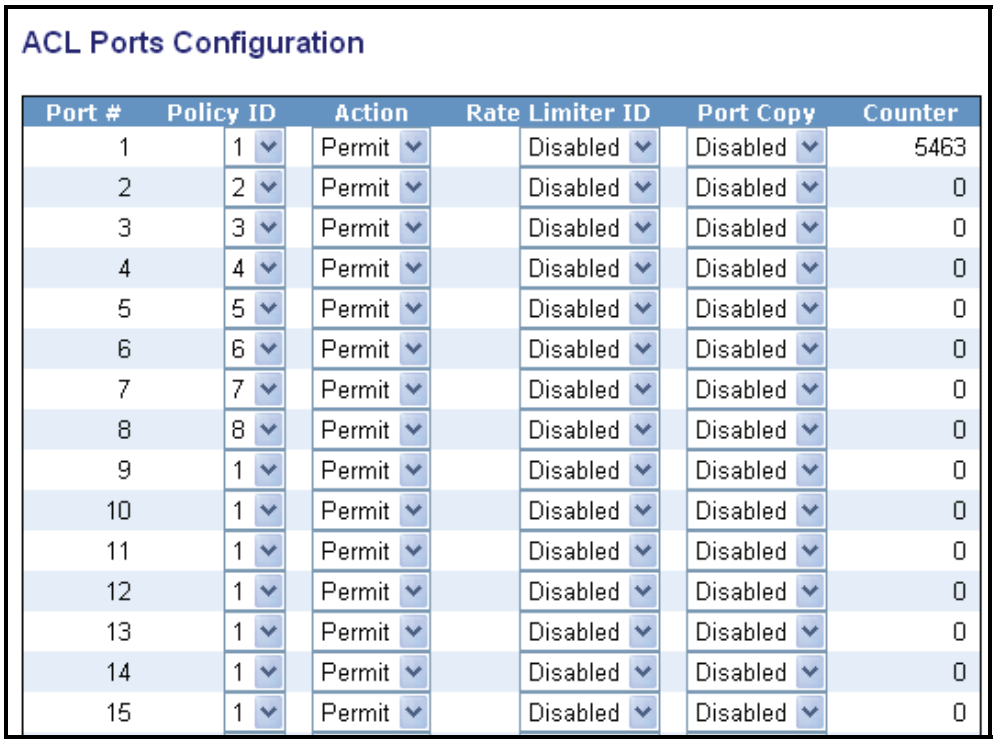

ACL Ports Configuration
Port # Policy ID Action Rate Limiter ID Port Copy Counter
1 1 Permit Disabled Disabled 5463
2 2 Permit Disabled Disabled 0
3 3 Permit Disabled Disabled 0
4 4 Permit Disabled Disabled 0
5 5 Permit Disabled Disabled 0
6 6 Permit Disabled Disabled 0
7 7 Permit Disabled Disabled 0
8 8 Permit Disabled Disabled 0
9 1 Permit Disabled Disabled 0
10 1 Permit Disabled Disabled 0
11 1 Permit Disabled Disabled 0
12 1 Permit Disabled Disabled 0
13 1 Permit Disabled Disabled 0
14 1 Permit Disabled Disabled 0
15 1 Permit Disabled Disabled 0

Fig. 3-133 Set up Port Policies Finish

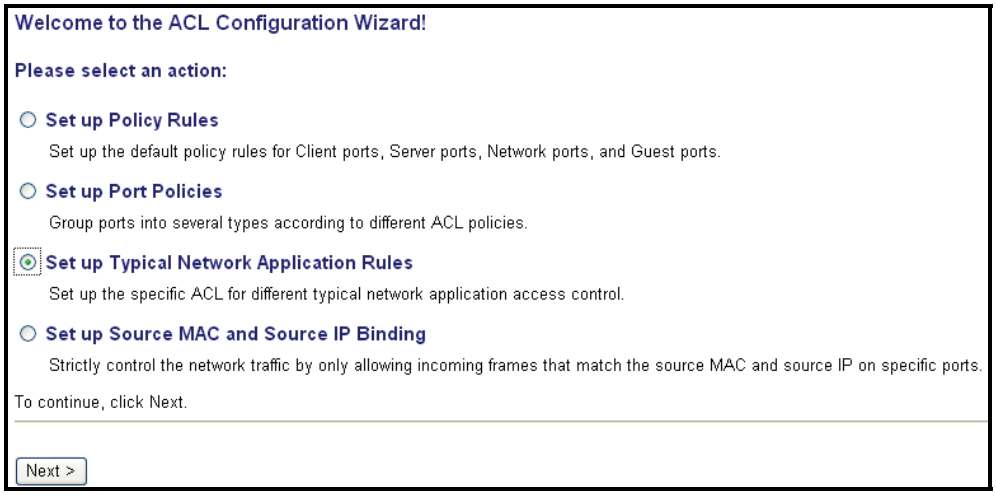
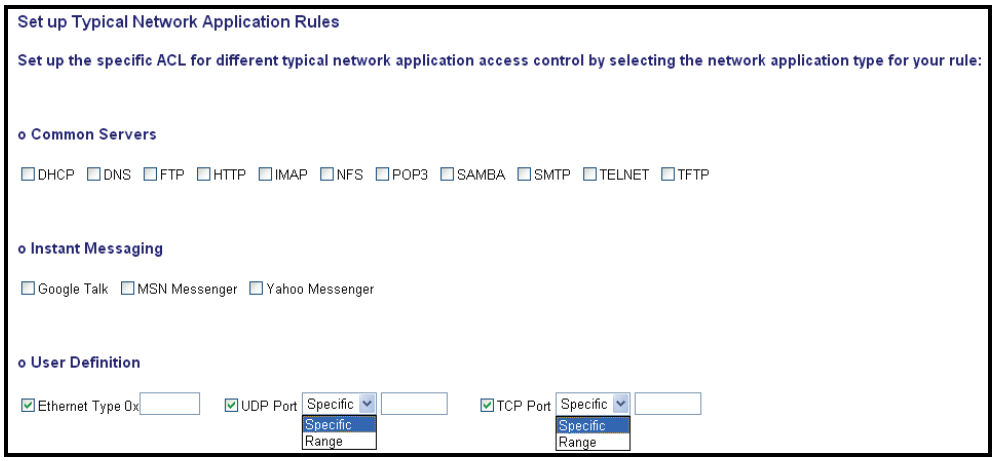

Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
To continue, click Next.
Next >

Fig. 3-134 Set up Typical Network Application Rules


Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control by selecting the network application type for your rule:
o Common Servers
DHCP DNS FTP HTTP IMAP NFS POP3 SAMBA SMTP TELNET TFTP
o Instant Messaging
Google Talk MSN Messenger Yahoo Messenger
o User Definition
Ethernet Type 0x
UDP Port Specific
TCP Port Specific
Specific
Range

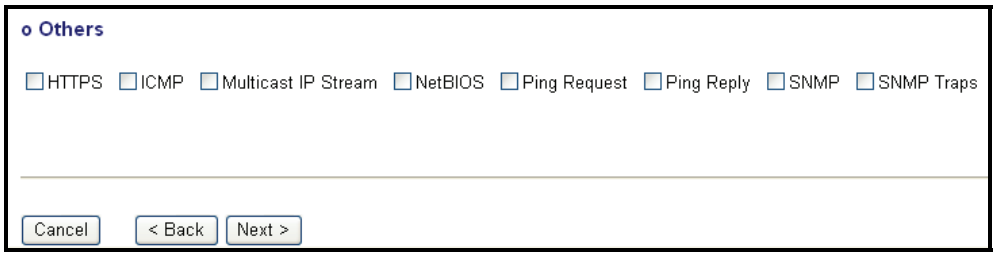


Fig. 3-135 Set up Typical Network Application Rules

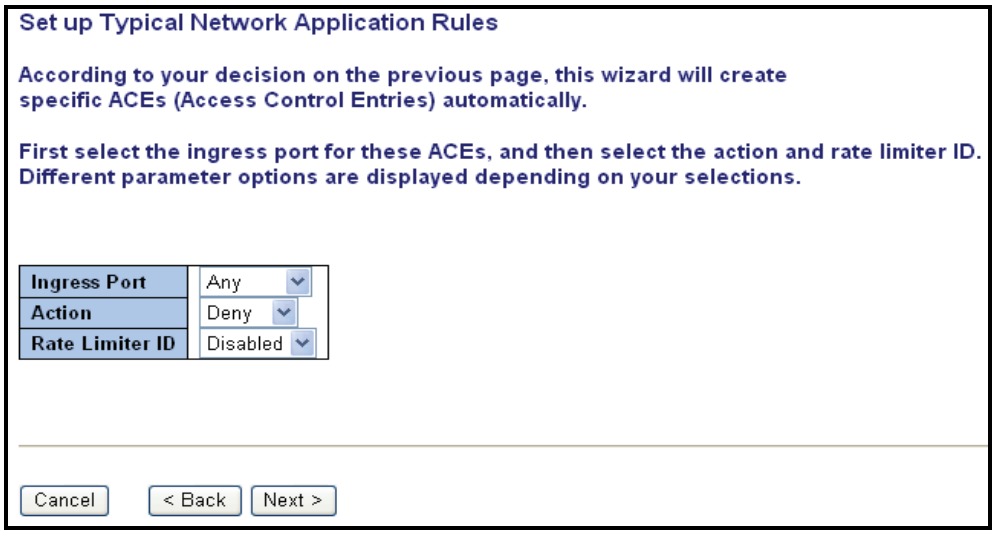

Set up Typical Network Application Rules
According to your decision on the previous page, this wizard will create specific ACEs (Access Control Entries) automatically.
First select the ingress port for these ACEs, and then select the action and rate limiter ID. Different parameter options are displayed depending on your selections.
Ingress Port
Any
Action
Deny
Rate Limiter ID
Disabled
Cancel
< Back
Next >

Fig. 3-136 Set up Typical Network Application Rules

Finished !
The ACL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-137 Set up Typical Network Application Rules

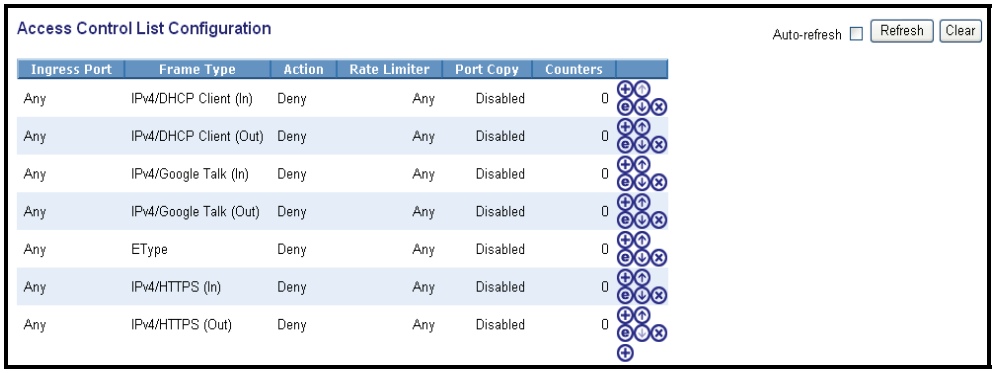

Access Control List Configuration
Auto-refresh
Refresh
Clear
Ingress Port
Frame Type
Action
Rate Limiter
Port Copy
Counters
Any IPv4/DHCP Client (In) Deny Any Disabled 0
Any IPv4/DHCP Client (Out) Deny Any Disabled 0
Any IPv4/Google Talk (In) Deny Any Disabled 0
Any IPv4/Google Talk (Out) Deny Any Disabled 0
Any EType Deny Any Disabled 0
Any IPv4/HTTPS (In) Deny Any Disabled 0
Any IPv4/HTTPS (Out) Deny Any Disabled 0

Fig. 3-138 Set up Typical Network Application Rules Finish

Parameter description:

Common Server:

DHCP / DNS / FTP / HTTP / IMAP / NFS / POP3 / SAMBA / SMTP / TELNET / TFTP

Instant Messaging:

Google Talk / MSN Messenger / Yahoo Messenger

User Definition:

Ethernet Type / UDP Port / TCP Port

Others:

TCP Port / ICMP / Multicast IP Stream / NetBIOS / Ping Request / Ping Reply / SNMP / SNMP Traps

Ingress Port:

Any / Policy1-8 / Port1-16

Action:

Permit / Deny

Rate Limiter ID:

Disabled / 1-16

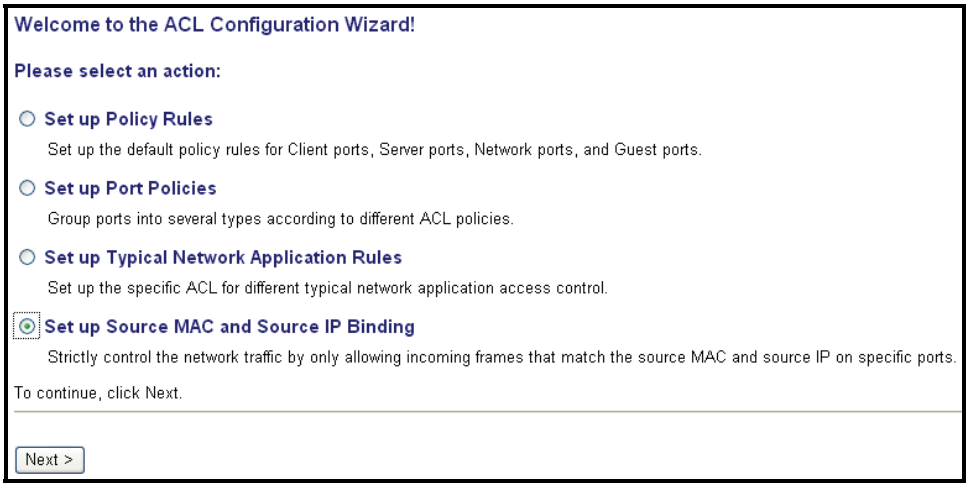

Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
To continue, click Next.
Next >

Fig. 3-139 Set up Source MAC and Source IP Binding

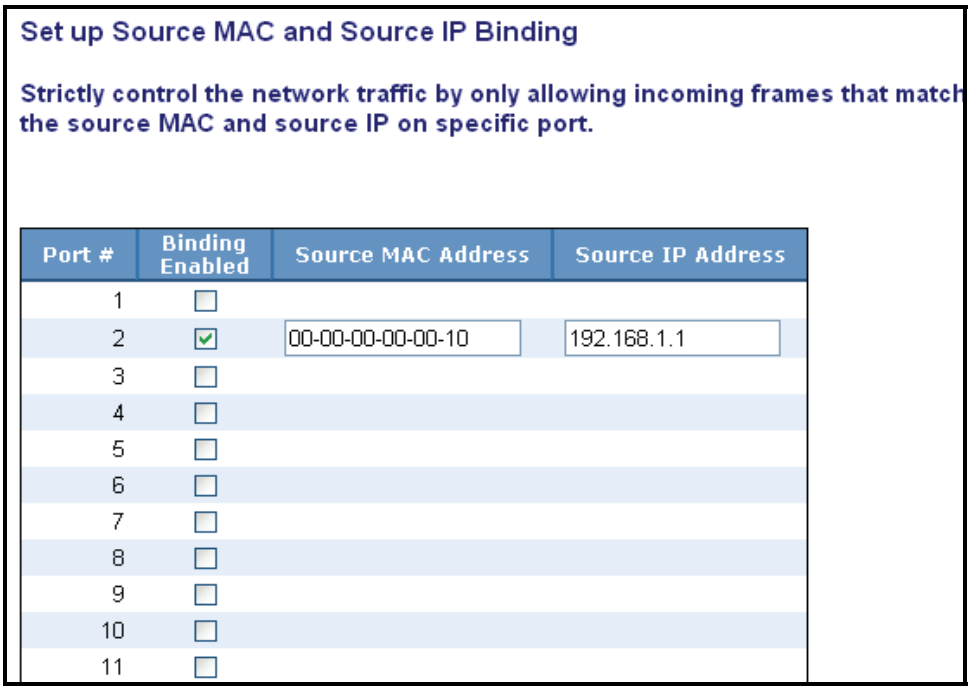


Fig. 3-140 Set up Source MAC and Source IP Binding

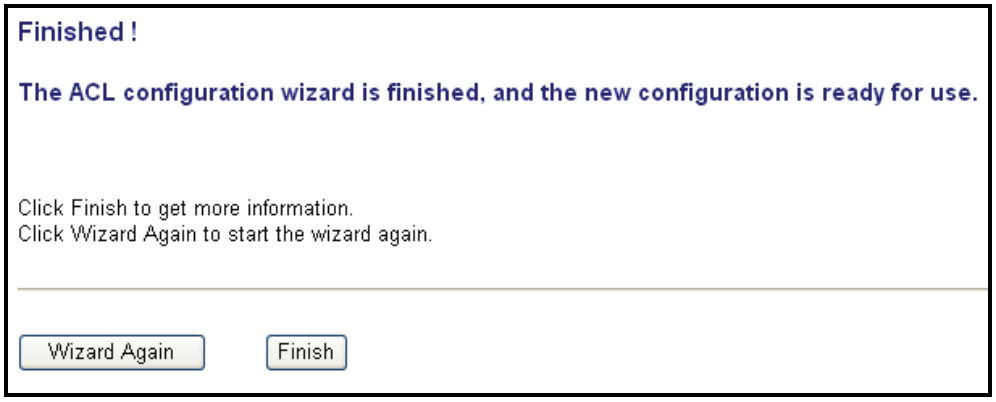

Finished !
The ACL configuration wizard is finished, and the new configuration is ready for use.
Click Finish to get more information.
Click Wizard Again to start the wizard again.
Wizard Again
Finish

Fig. 3-141 Set up Source MAC and Source IP Binding

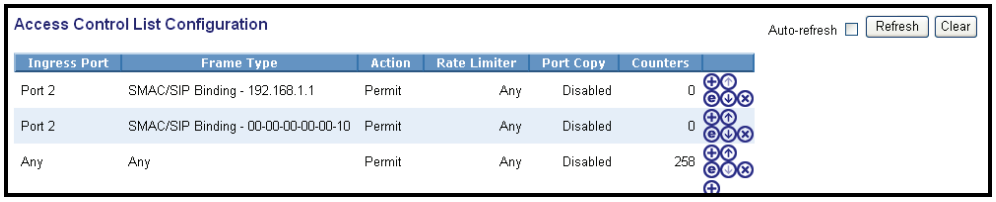


Fig. 3-142 Set up Source MAC and Source IP Binding Finish

Parameter description:

Port #:

1-16

Binding Enabled:

Use the switch ACL function to support IP/MAC Binding function, the maximum is up to 128 entries.

Source MAC Address: xx-xx-xx-xx-xx-xx

For example: 00-40-c7-00-00-01

Source IP Address: xxx.xxx.xxx.xxx

For example: 192.168.1.100

3-9. IP MAC Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

Function name:

IP MAC Binding Configuration

Function description:

The switch has client and server classes of IP-MAC Binding table. The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries. The creation of authorized users can be done manually. The function is global, this means a user can enable or disable the function for all ports on the switch.

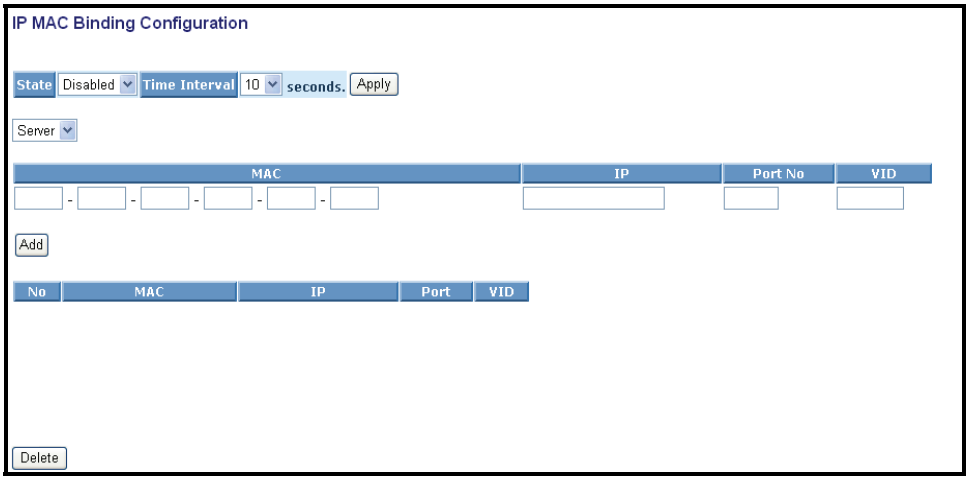


Fig. 3-143

Parameters description:

State:

Disabled / Enabled

Time Interval:

Range: 10 / 20 / 30

Time interval is for ARP echo, the switch will send ARP echo according to server table entries.

Server/Client:

The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries.

MAC:

Six-byte MAC Address: xx-xx-xx-xx-xx-xx

For example: 00-40-c7-00-00-01

IP:

Four-byte IP Address: xxx.xxx.xxx.xxx

For example: 192.168.1.100

Port No:

Port no.: 1-16

VID:

VLAN ID: 1-4094

Add:

Input MAC, IP, Port and VID, then click on <Add> to create a new entry into the IP MAC Binding table

Delete:

Select one entry from the table, then click on <Delete> to delete this entry.

3-10. 802.1X Configuration

802.1X port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1X-enabled port without authentication. If a user wishes to access the network through a port under 802.1X control, he/she must first input his/her account name for authentication and wait for authorization before sending or receiving any packets from a 802.1X-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1X control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator passes the request to the authentication server to authenticate and verify, and the server tells the authenticator if the request is granted authorization for the ports.

According to IEEE802.1X, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 3-53.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE requests it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE.

The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once re-authenticating is started the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with a PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for Fig. 3-53 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchange an authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only access the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

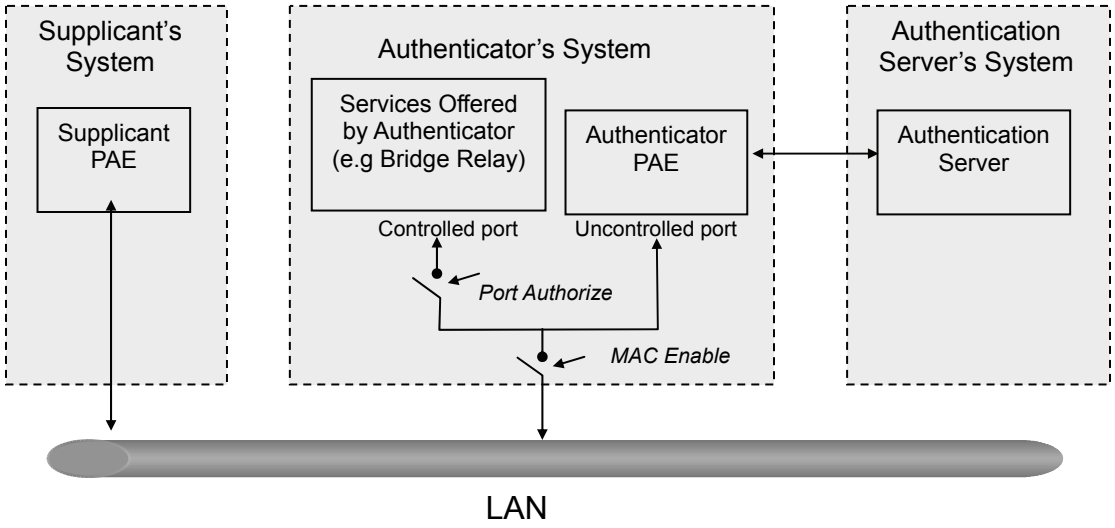
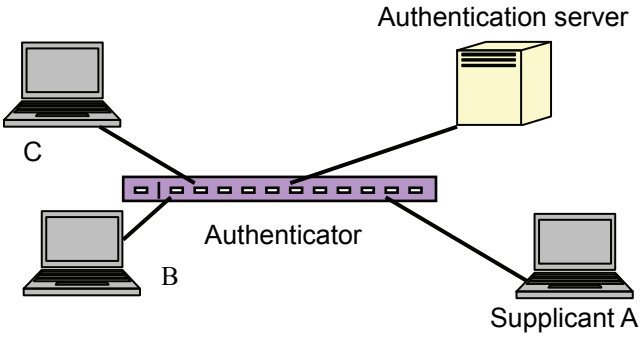


Fig. 3-53

In Fig. 3-54, this is the typical configuration. A single supplicant, an authenticator and an authentication server. B and C are in the internal network, D is Authentication server running RADIUS, a switch at the central location acts as Authenticator connecting to PC A and A is a PC outside the controlled port running Supplicant PAE. In this case, if PC A wants to access the services on device B and C, first it must exchange the authentication message with the authenticator on the port it is connected to via EAPOL packet. The authenticator transfers the supplicant's credentials to the Authentication server for verification. If successful, the authentication server will authenticate the grant. PC A is then allowed to access B and C via the switch. If there are two switches directly connected together instead of a single one, for the link connecting two switches, it may have to assume two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

Fig. 3-54



The Fig. 3-55 shows the procedure of 802.1X authentication. There are steps for the login based on 802.1X port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.

2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond to EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.

4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Starting the process by sending to the authenticator.

5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.

6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant asking for the user password via the authenticator PAE.

7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and reply an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.

8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1X control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant has failed to authenticate. If the port connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issues an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.

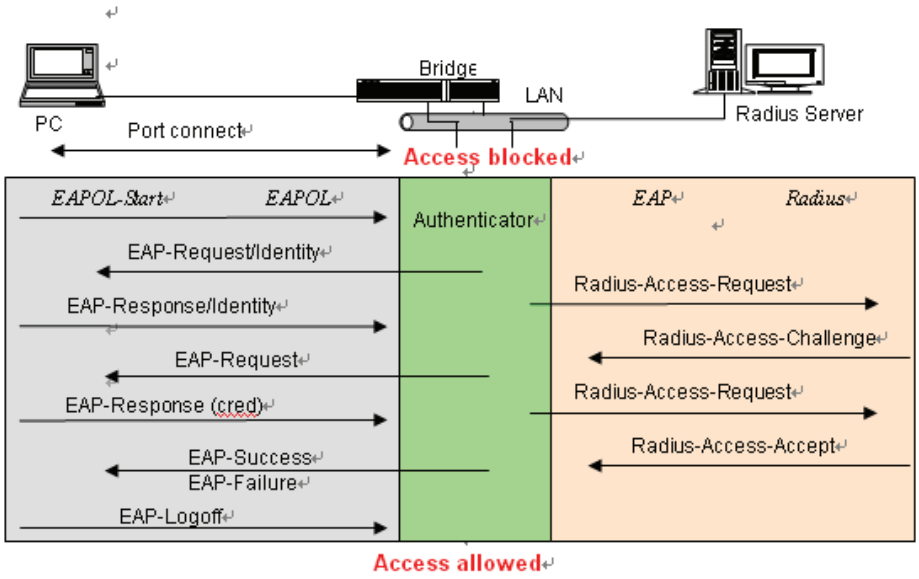


Fig. 3-55

Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1X Port-based Network Access Control function supported by the switch is a bit complex, for it just supports basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1X Port mode, port control state, set in 802.1X port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

Table 3-3

3-10-1.Server

Function name:

802.1X Server Configuration

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1X port security application.

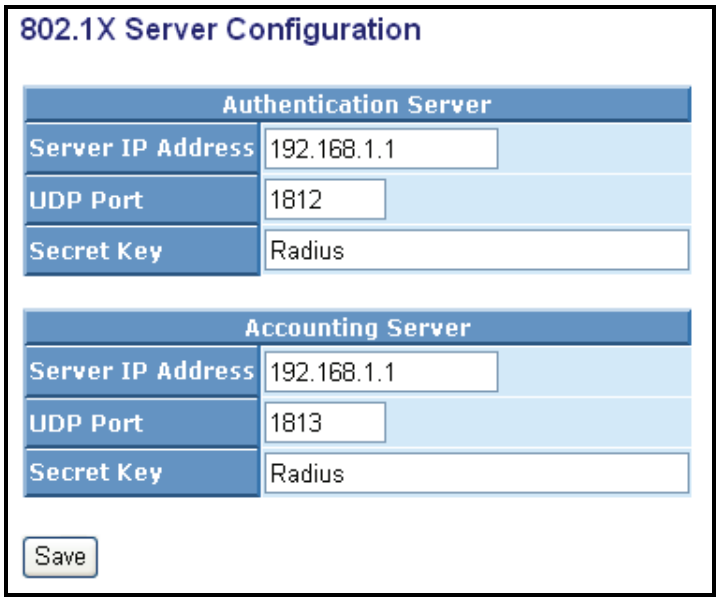


Fig. 3-144

Parameter description:

Authentication Server

Server IP Server:

Server IP address for authentication.

Default: 192.168.1.1

UDP Port:

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sensitive. Blanks are not permitted between any two characters.

Default: Radius

Accounting Server

Server IP Server:

Server IP address for authentication.

Default: 192.168.1.1

UDP Port:

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length

1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. Blanks are not permitted between any two characters.

Default: Radius

3-10-2.Port Configuration

Function name:

802.1X Port Configuration

Function description:

This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.

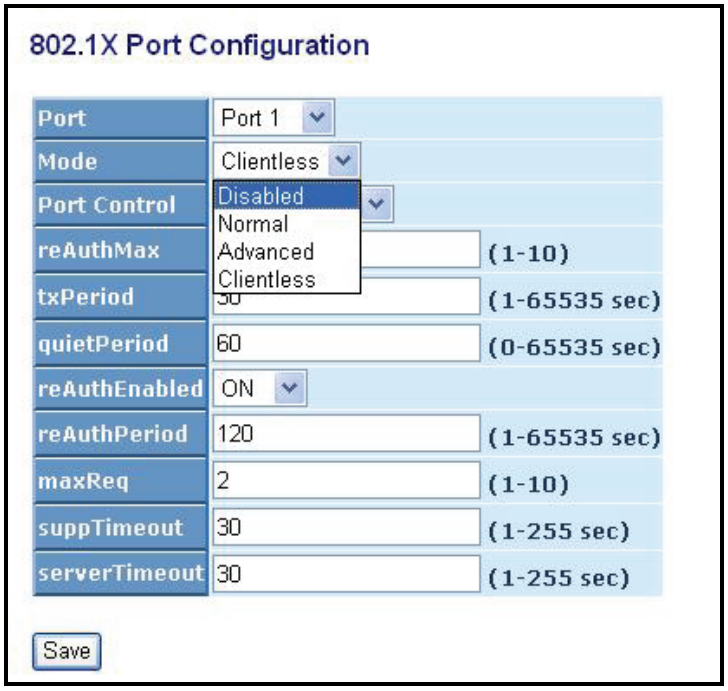


Fig. 3-145

Parameter description:

Port:

It is the port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Mode:

Range: Disable / Normal / Advanced / Clientless

Disable:

Disable IEEE 802.1X for this port.

Normal:

All clients under this port will be authorized when one of the clients is 802.1X authenticated.

Advanced:

Each client under this port has to acquire 802.1X authentication individually.

Clientless:

The clients don't need to install the 802.1X client function. This means the client PC (for example WINDOW XP) does not need to enable 802.1X client function for 802.1X authentication. But the network maintainer needs to configure the Radius server using each client's MAC address for Radius account ID and password.

Port Control:

This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

- ForceUnauthorized:

  The controlled port is forced to hold in the unauthorized state.

- ForceAuthorized:

  The controlled port is forced to hold in the authorized state.

- Auto:

  The controlled port is set to an authorized state or unauthorized state depending on the result of the authentication exchange between the authentication server and the supplicant.

  Default: Auto

reAuthMax(1-10):

The number of authentication attempts permitted before the port becomes unauthorized.

Default: 2

txPeriod(1-65535 s):

A time period transmitted EAPOL PDU between the authenticator and the supplicant.

Default: 30

Quiet Period(0-65535 s):

A period of time during which access to the supplicant will not be attempted.

Deafult: 60 seconds

reAuthEnabled:

Choose whether regular authentication will take place in this port.

Default: ON

reAuthPeriod(1-65535 s):

A non-zero number of seconds between the periodic re-authentication of the supplicant.

Default: 3600

max. Request(1-10):

The maximum number of times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

Default: 2 times

suppTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –65535.

Default: 30 seconds.

serverTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

Default: 30 seconds

3-10-3.Status

Function name:

802.1X Status

Function description:

Show each port IEEE 802.1X authentication current operating mode and status.

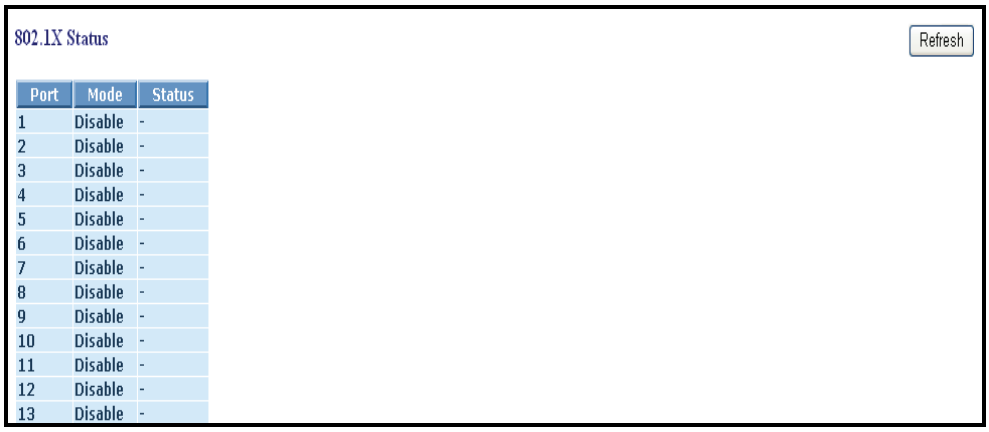


Fig. 3-146

Parameter description:

Port:

Port number: 1-16

Mode:

Show the port IEEE 802.1X operating mode: There are four modes Disable, Normal, Advance and Clientless

Status:

Show the port IEEE 802.1X security current status: Authorized or Unauthorized

3-10-4. Statistics

Function name:

802.1X Port Statistics Port1

Function description:

Show the IEEE 802.1X authentication related counters for manager monitoring authenticator status.

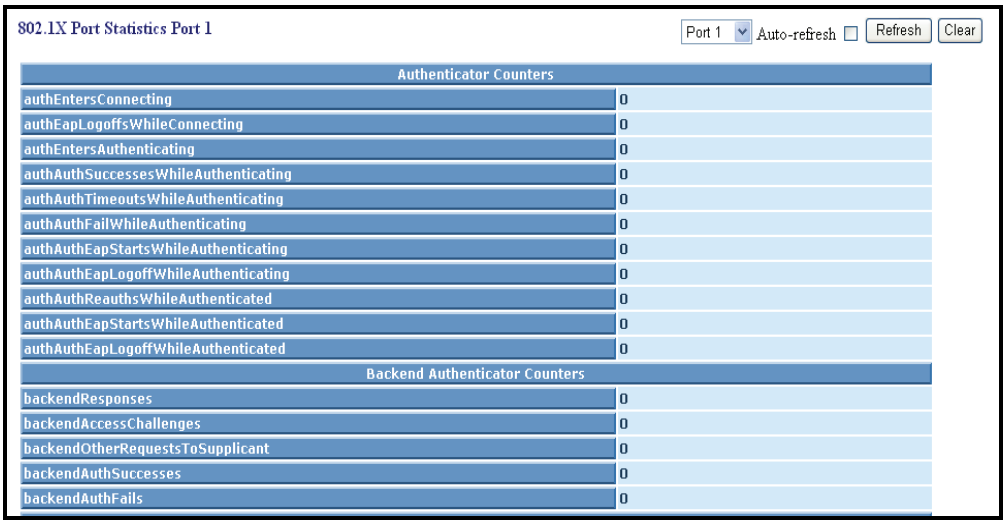


Fig. 3-147

Parameter description:

Port:

Port Number: 1-16

Auto - refresh:

Refresh the authenticator counters in the web UI automatically

Refresh:

Click on the <Refresh> to update the authenticator counters in the web UI

Clear:

Click on the <Clear> to clear all authenticator counters in the web UI

3-11. Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port.

The switch supports two kinds of port trunking methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~8) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregating ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~8, this Static groupID can be the same with another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a “logic trunked port”. Using Static Trunk on both ends of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch,
In the management point of view, the switch supports maximum 8 trunk groups for LACP and additional 8 trunk groups for Static Trunk. But in the system capability view, only 8 “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

Per Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

a) 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the “None” trunking method and its Group ID will turn to 0. This means the port won’t aggregate with other ports.

b) 14 ports all use LACP Trunk Group ID 1. At most 12 ports can aggregate together and transit into the ready state.

c) A port using the “None“ trunking method or Group ID 0 will be automatically set to use the “None” trunking method with Group ID 0.

3-11-1.Port

Function name:

Trunk Port Setting/Status

Function description:

Port setting/status is used to configure the trunk property of each and every port in the switch system.

Trunk Port Setting/Status

Trunk Port Setting				Trunk Port Status	
Port	Method	Group	Active LACP	Aggtr	Status
1	None	0	Active	1	Ready
2	None	0	Active	2	---
3	None	0	Active	3	---
4	None	0	Active	4	---
5	None	0	Active	5	---
6	None	0	Active	6	---
7	None	0	Active	7	---
8	None	0	Active	8	---
9	None	0	Active	9	---
10	None	0	Active	10	---
11	None	0	Active	11	---
12	None	0	Active	12	---
13	None	0	Active	13	---
14	None	0	Active	14	---
15	None	0	Active	15	---

Fig.3-148

Parameter description:

Port:

Port Number: 1-16

Method:

This determines the method a port uses to aggregate with other ports.

None:

Select this default setting if port aggregation is not required.

LACP:

Select this setting if using the LACP trunking method with other ports also using LACP.

Static:

Select this setting if using the Static Trunk method with other ports also using Static Trunk.

Group:

Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.

Active LACP:

This field is only referenced when a port’s trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity starts to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr:

Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status:

This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”

3-11-2 Aggregator View

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.

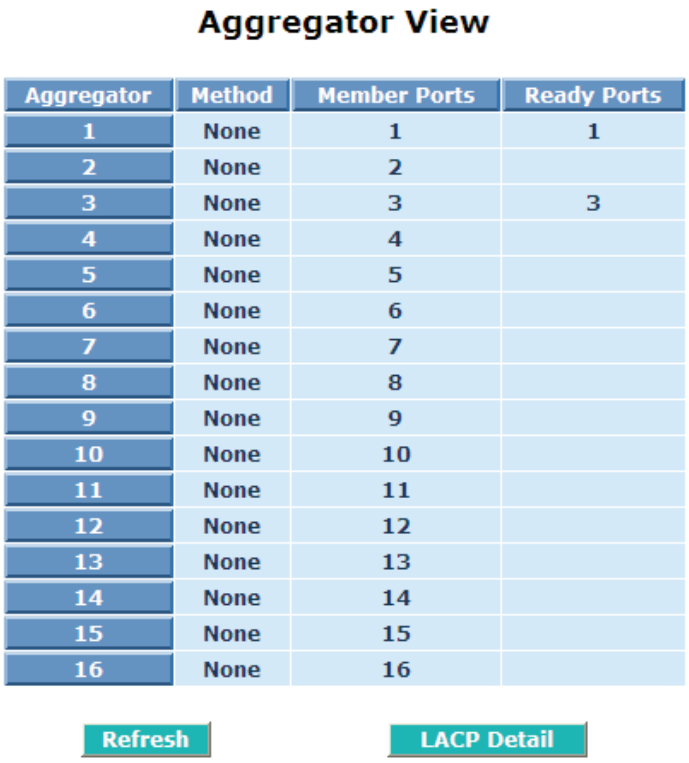


Fig.3-149

Parameter description:

Aggregator:

It shows the aggregator ID (from 1 to 16) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

Method:

Shows the method a port uses to aggregate with other ports.

Member Ports:

Shows all member ports of an aggregator (port).

Ready Ports:

Shows only the ready member ports within an aggregator (port).

3-11-3 LACP System Priority

Function name:

LACP System Priority

Function description:

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supporting LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768

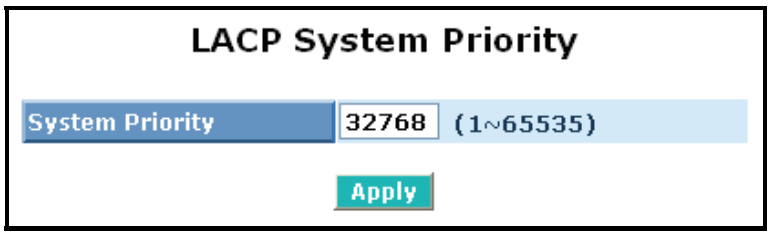


Fig. 3-150

Parameter description:

System Priority:

Shows the System Priority part of a system ID.(1-65535)

3-12 STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

3-12-1 STP Status

Function name:

STP Status

Function description:

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.

STP Status

STP State	Disabled
Bridge ID	00:40:C7:5D:00:01
Bridge Priority	32768
Designated Root	00:40:C7:5D:00:01
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	0

Fig. 3-151

Parameter description:

STP State:

Shows the current STP Enabled / Disabled status. Default is "Disabled".

Bridge ID:

Shows switch's bridge ID which stands for the MAC address of this switch.

Bridge Priority:

Shows this switch's current bridge priority setting. Default is 32768.

Designated Root:

Shows root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority:

Shows the current root bridge priority.

Root Port:

Shows port number connected to root bridge with the lowest path cost.

Root Path Cost:

Shows the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Shows the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge as malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine the root bridge. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Current Forward Delay:

Shows the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state to Learning state or from Learning state to Forwarding state of a port in the bridge.

Hello Time:

Shows the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request that all other bridges periodically send a hello message every “hello time” seconds to the bridge attached to its designated port.

STP Topology Change Count:

STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close.

Time Since Last Topology Change:

Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

3-12-2. Configuration

The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure. Each parameter description is listed below.

Function name:

STP Configuration

Function description:

User can set the following Spanning Tree parameters to control STP function, enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is “Disable”.

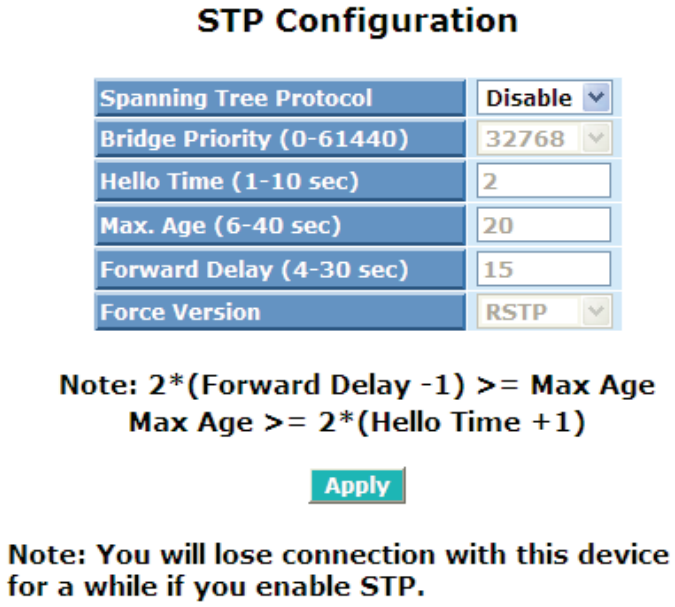


Fig. 3-152

Parameter description:

Spanning Tree Protocol:

Set 802.1W Rapid STP function Enable / Disable. Default is “Disable”

Bridge Priority:

The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the SG71660MA as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

Hello Time:

Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridges to sayl I am alive. When the SG71660MA is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.

Default is 2 seconds.

Max. Age:

When the SG71660MA is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge receives a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge as malfunctioning and issue a Topology Change Notification

(TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

Forward Delay:

You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state to Learning state and also from Learning state to Forwarding state of a port on the bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This is associated with the STP convergent time which will be more than 30 seconds because of some other factors.

The valid value is 4 ~ 30 seconds, default is 15 seconds.

Force Version:

Two STP algorithm options are offered for the user. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

3-12-3. STP Port Configuration

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameter settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.

STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	FORWARDING	2000000	0	128	Normal	Auto
2	FORWARDING	2000000	0	128	Normal	Auto
3	FORWARDING	2000000	0	128	Normal	Auto
4	FORWARDING	2000000	0	128	Normal	Auto
5	FORWARDING	2000000	0	128	Normal	Auto
6	FORWARDING	2000000	0	128	Normal	Auto
7	FORWARDING	2000000	0	128	Normal	Auto
8	FORWARDING	2000000	0	128	Normal	Auto
9	FORWARDING	2000000	0	128	Normal	Auto
10	FORWARDING	2000000	0	128	Normal	Auto
11	FORWARDING	2000000	0	128	Normal	Auto
12	FORWARDING	2000000	0	128	Normal	Auto
13	FORWARDING	2000000	0	128	Normal	Auto
14	FORWARDING	2000000	0	128	Normal	Auto
15	FORWARDING	2000000	0	128	Normal	Auto
16	FORWARDING	2000000	0	128	Normal	Auto

Edit MCheck

Fig. 3-153

Parameter description:

Port Status:

It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

- DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

- LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets.

- FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status:

It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

Configured Path Cost:

The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulting from auto-negotiation of the link and display this value in the

field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

10 Mbps : 2,000,000

100 Mbps : 200,000

1 Gbps : 20,000

Default: 0

Priority:

Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

Default is 128.

Admin Edge Port:

If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transition to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point To Point:

We say a port is a point-to-point link, from RSTP’s view, if it is in full-duplex mode but is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will transition the port quickly to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If this parameter is set to Auto, it means RSTP will use the duplex mode resulting from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not transition quickly to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

Default: Auto

M Check:

Migration Check. It forces the port to send out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click **<M Check>** button to send a RSTP BPDU from the port you specified.

3-13 MSTP

The implementation of MSTP is according to IEEE 802.1Q 2005 Clause 13 – Multiple Spanning Tree Protocol. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. Proper configuration of MSTP in an 802.1Q VLAN environment can ensure a loop-free data path for a group of vlans within an MSTI. Redundant path and load balancing in vlan environment is also achieved via this feature.A spanning tree instance called CIST(Common and Internal Spanning Tree) always exists . Up to 64 more spanning tree instances (MSTIs) can be provisioned.

3-13-1 Status

Function name:

MSTP State

Function description:

To enable or disable MSTP and to select a version of Spanning Tree protocol under which MSTP should operate.

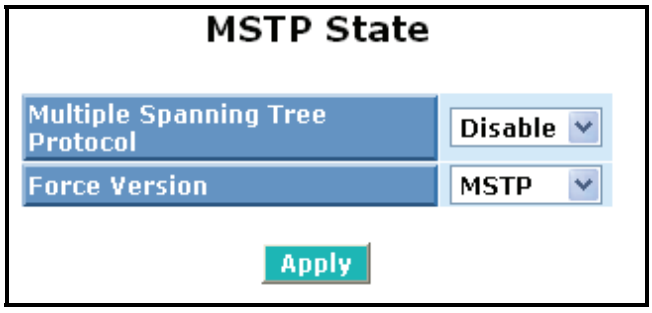


Fig. 3-154

Parameter description:

Multiple Spanning Tree Protocol:

Disabled / Enabled

Force Version:

STP / RSTP / MSTP

3-13-2 Region Config

Function name:

MSTP Region Config

Function description:

To configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

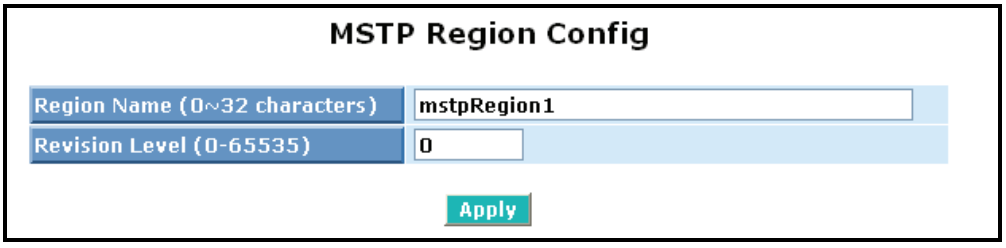


Fig. 3-155

Parameter description:

Region Name:

0-32 characters.(A variable length text string encoded within a fixed field of 32 octets , conforming to RFC 2271's definition of SnmpAdminString.)

Revision Level:

0-65535

3-13-3 Instance View

(Fig. 3-156)

Function name:

MSTP Instance Config

Function description:

Providing an MST instance table which includes information(vlan membership of a MSTI) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

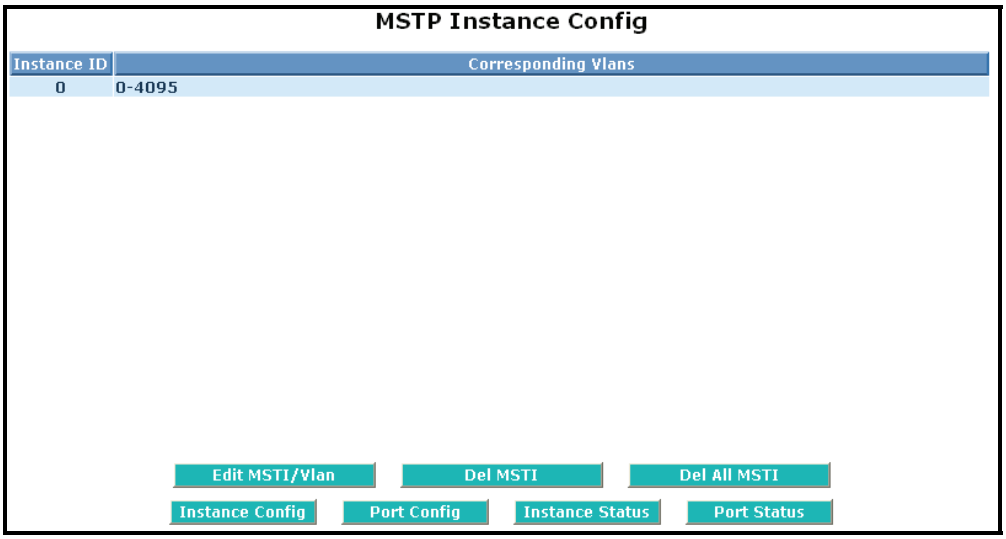


Fig. 3-156

Parameter description:

Instance ID:

Every spanning tree instance need to have a unique instance ID within 0~4095. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.

Corresponding Vlans:

0-4095.

Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).

Edit MSTI / Vlan: ***Fig. 3-157***

To add an MSTI and provide its vlan members or modify vlan members for a specific MSTI.

Del MSTI:

To delete an MSTI.

Del All MSTI:

Deleting all provisioned MSTIs at a time.

Instance Configuration: ***Fig. 3-158***

To provision spanning tree performance parameters per instance.

Port Config: ***Fig. 3-159***

To provision spanning tree performance parameters per instance per port.

Instance Status: ***Fig. 3-160***

To show the status report of a particular spanning tree instance.

Port Status: ***Fig. 3-161***

To show the status report of all ports regarding a specific spanning tree instance.

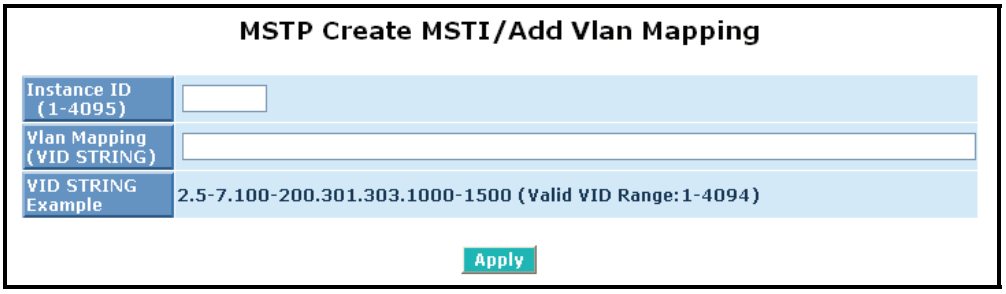


Fig. 3-157 Edit MSTI / Vlan

Parameter description:

Vlan Mapping:

VID STRING

VID STRING Example:

2.5-7.100-200.301.303.1000-1500 (Valid VID Range:1-4094)

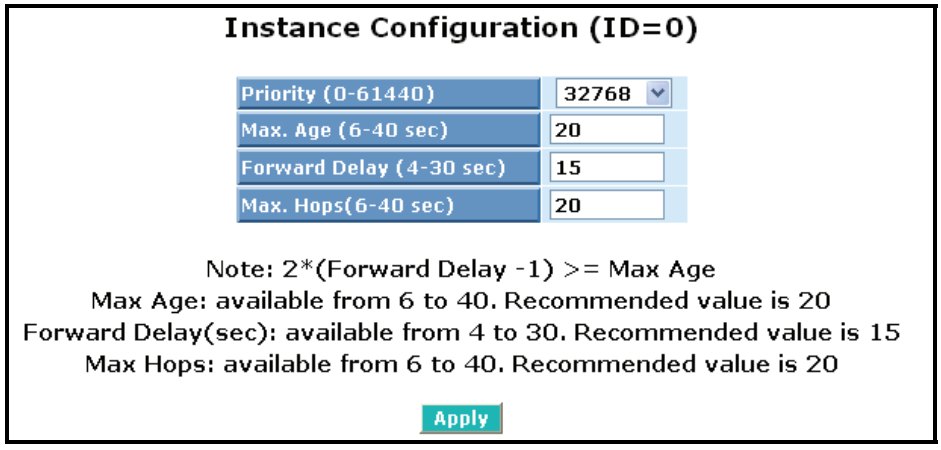

Instance Configuration (ID=0)
Priority (0-61440)
32768
Max. Age (6-40 sec)
20
Forward Delay (4-30 sec)
15
Max. Hops(6-40 sec)
20
Note: 2*(Forward Delay -1) >= Max Age
Max Age: available from 6 to 40. Recommended value is 20
Forward Delay(sec): available from 4 to 30. Recommended value is 15
Max Hops: available from 6 to 40. Recommended value is 20
Apply

Fig. 3-158 Instance Config

Parameter description:

Priority: The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

MAX. Age:

6-40sec. The same definition as in the RSTP protocol.

Forward Delay:

4-30sec. The same definition as in the RSTP protocol.

MAX. Hops:

6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal

spanning tree instances. “CIST Remaining Hops” or “MSTI Remaining Hops” in the Spanning tree protocol message would decrease by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)

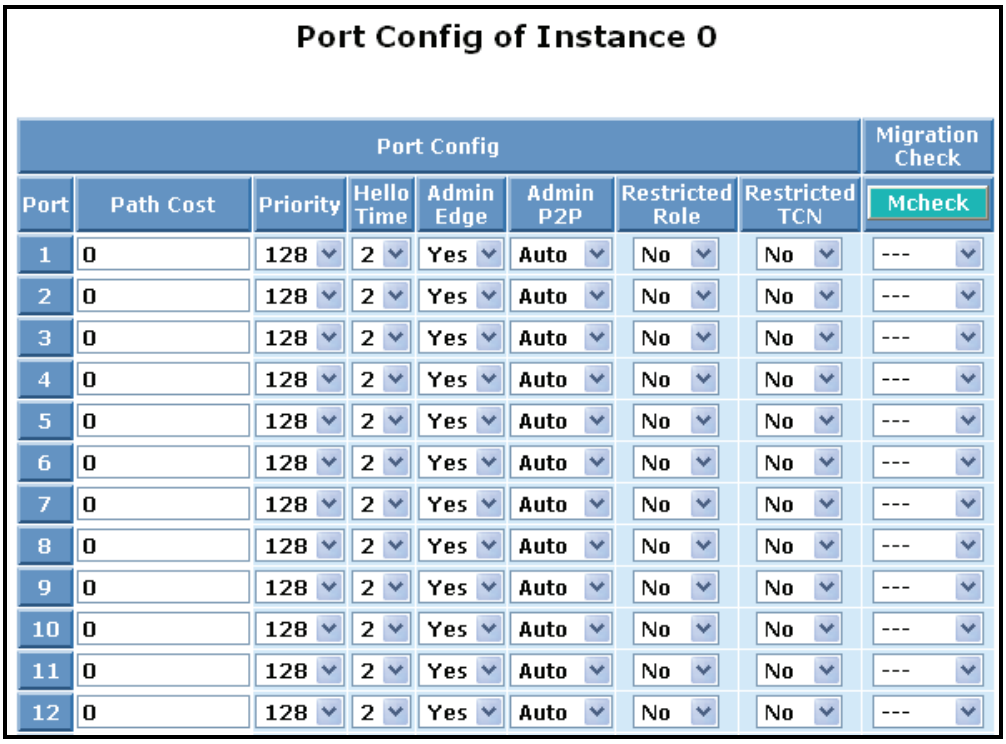

Port Config of Instance 0
Port Config
Migration Check
Port
Path Cost
Priority
Hello Time
Admin Edge
Admin P2P
Restricted Role
Restricted TCN
Mcheck
1 0 128 2 Yes Auto No No ---
2 0 128 2 Yes Auto No No ---
3 0 128 2 Yes Auto No No ---
4 0 128 2 Yes Auto No No ---
5 0 128 2 Yes Auto No No ---
6 0 128 2 Yes Auto No No ---
7 0 128 2 Yes Auto No No ---
8 0 128 2 Yes Auto No No ---
9 0 128 2 Yes Auto No No ---
10 0 128 2 Yes Auto No No ---
11 0 128 2 Yes Auto No No ---
12 0 128 2 Yes Auto No No ---

Fig. 3-159 Port Config

Parameter description:

Port:

1-16

Path Cost:

1 – 200,000,000

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Priority:

0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Hello Time:

1 / 2

In contrast with RSTP, Hello Time in MSTP is a per port setting for the CIST.

Admin Edge:

Yes / No

The same definition as in the RSTP specification for the CIST ports.

Admin P2P:

Auto / True / False

The same definition as in the RSTP specification for the CIST ports.

Restricted Role:

Yes / No

If "Yes" causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is "No" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

Restricted TCN:

Yes / No

If "Yes" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "No" by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. or the status of MAC operation for the attached LANs transitions frequently.

Mcheck:

The same definition as in the RSTP specification for the CIST ports.

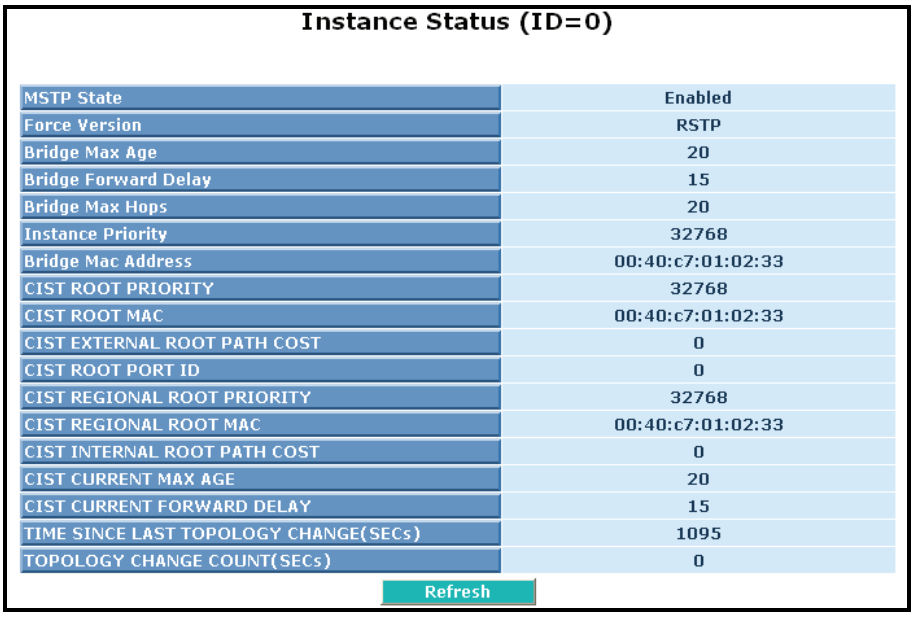


Fig. 3-160 Instance Status

Parameter description:

MSTP State:

MSTP protocol is Enable or Disable.

Force Version:

It shows the current spanning tree protocol version configured.

Bridge Max Age:

It shows the Max Age setting of the bridge itself.

Bridge Forward Delay:

It shows the Forward Delay setting of the bridge itself.

Bridge Max Hops:

It shows the Max Hops setting of the bridge itself.

Instance Priority:

Spanning tree priority value for a specific tree instance(CIST or MSTI)

Bridge Mac Address:

The Mac Address of the bridge itself.

CIST ROOT PRIORITY:

Spanning tree priority value of the CIST root bridge

CIST ROOT MAC:

Mac Address of the CIST root bridge

CIST EXTERNAL ROOT PATH COST:

Root path cost value from the point of view of the bridge's MST region.

CIST ROOT PORT ID:

The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in defferent MST region or in the same MST region.The first case indicates that the root port's owner is the CIST regional root bridge.

CIST REGIONAL ROOT PRIORITY:

Spanning tree priority value of the CIST regional root bridge.Note that CIST Regional Root bridge is different from CIST Root bridge.One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST(Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge.The IST(Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

CIST REGIONAL ROOT MAC:

Mac Address of the CIST regional root bridge.

CIST INTERNAL ROOT PATH COST:

Root path cost value from the point of view of the bridges inside the IST.

CIST CURRENT MAX AGE:

Max Age of the CIST Root bridge.

CIST CURRENT FORWARD DELAY:

Forward Delay of the CIST Root bridge.

TIME SINCE LAST TOPOLOGY CHANGE(SECs):

Time Since Last Topology Change is the elapsed time in unit of seconds for several "Topology Change and(or) Topology Change Notification receiving" to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

TOPOLOGY CHANGE COUNT(SECs):

The per spanning tree instance Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

Port Status of Instance 0

Refresh

Port No	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P	Restricted Role	Restricted Tcn
1	FORWARDING	DSGN	200000	128	2/2	V	V		
2	DISCARDING	dsbl	2000000	128	2/2	V			
3	FORWARDING	ROOT	200000	128	2/2		V		
4	DISCARDING	dsbl	2000000	128	2/2	V			
5	DISCARDING	dsbl	2000000	128	2/2	V			
6	DISCARDING	dsbl	2000000	128	2/2	V			
7	DISCARDING	dsbl	2000000	128	2/2	V			
8	DISCARDING	dsbl	2000000	128	2/2	V			
9	DISCARDING	dsbl	2000000	128	2/2	V			
10	DISCARDING	dsbl	2000000	128	2/2	V			
11	DISCARDING	dsbl	2000000	128	2/2	V			
12	DISCARDING	dsbl	2000000	128	2/2	V			
13	DISCARDING	dsbl	2000000	128	2/2	V			
14	DISCARDING	dsbl	2000000	128	2/2	V			
15	DISCARDING	dsbl	2000000	128	2/2	V			
16	DISCARDING	dsbl	2000000	128	2/2	V			

Refresh

Fig. 3-161 Port Status

Parameter description:

Port No:

1-16

Status:

The forwarding status.Same definition as of the RSTP specification Possible values are “FORWARDING” , “LEARNING” , “DISCARDING”

Status:

The role that a port plays in the spanning tree topology. Possible values are “dsbl”(disable port) , ”alt”(alternate port) , “bkup”(backup port) , “ROOT”(root port) , “DSGN”(designated port) , “MSTR”(master port). The last 3 are possible port roles for a port to transit to FORWARDING state

Path Cost:

Display currently resolved port path cost value for each port in a particular spanning tree instance.

Priority:

Display port priority value for each port in a particular spanning tree instance.

Hello:

Per port Hello Time display. It takes the following form:

Current Hello Time/Hello Time Setting

Oper. Edge:

Whether or not a port is an Edge Port in reality.

Oper. P2P:

Whether or not a port is a Point-to-Point Port in reality.

Restricted Role:

Same as mentioned in “Port Config”

Restricted Tcn:

Same as mentioned in “Port Config”

3-14. Mirror

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Note: When configuring the mirror function, you should avoid setting a port to be a sniffer port and aggregated port at the same time.

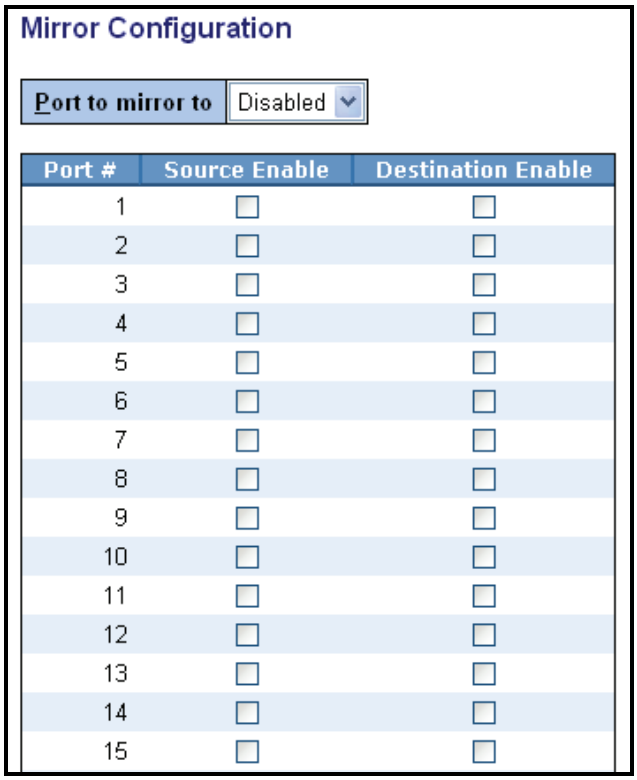


Fig. 3-162

Parameter description:

Port to mirror to:

Range: Disabled / Port 1-16

Set the monitoring port.

Port #:

Range: 1-16

Select the monitored ports.

Source Enable:

The source enable means the monitored port ingress traffic will be copied to monitoring port.

Destination Enable:

The destination enable means the monitored port egress traffic will be copied to monitoring port.

3-15. IGMP Snooping

The function IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supporting IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance.

3-15-1 Proxy

Function name:

IGMP Proxy Configuration

Function description:

IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts as a *proxy* for its hosts.

You enable IGMP proxy on the switch, which connects to a router closer to the root of the tree. This interface is the *upstream interface*. The router on the upstream interface should be running IGMP.

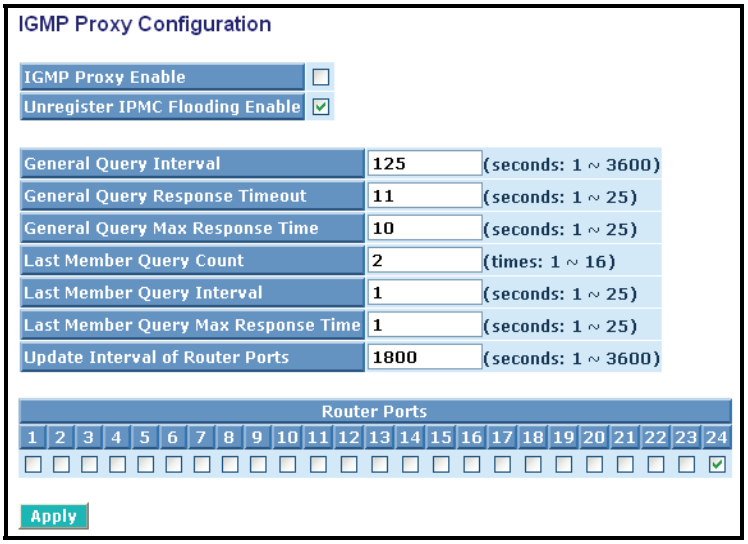


Fig. 3-163 IGMP Proxy

Parameter description:

IGMP snooping mode selection:

The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

Disable:

Set “Disable” mode to disable IGMP Snooping function.

Default: Disable

Active:

In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic.

Passive:

In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address:

Show all multicast groups IP addresses that are registered on this device.

VLAN ID:

Show VLAN ID for each multicast group.

Member Port:

Show member ports that join each multicast group. Member port may be only or more than one.

3-15-2 Group Membership

Function name:

Group Membership

Function description:

To show the IGMP group members information, the you can edit the parameters for IGMP groups and members in the web user interface.

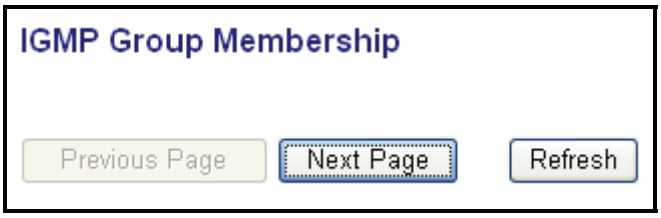


Fig. 3-164

Parameter description:

IP Range:

The switch supports two kinds of options for managed valid IP range, including “Any” and “Custom”. Default is “Any”. In case that” Custom” had been chosen, you can assigned effective IP range. The valid range is 224.0.0.0~239.255.255.255.

VID:

The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom”. Default is “Any”. When you choose “Custom”, you can fill in VID number. The valid VID range is 1~4094.

Port:

The switch supports two kinds of options for managed valid port range, including “Any” and “Custom”. Default is “Any”. You can select the ports that you would like them to be worked and restricted in the allowed group configuration if ”Custom” had been chosen.

Add:

A new entry of allowed group configuration can be created after the parameters as mentioned above had been setup and then press **<Add>** button.

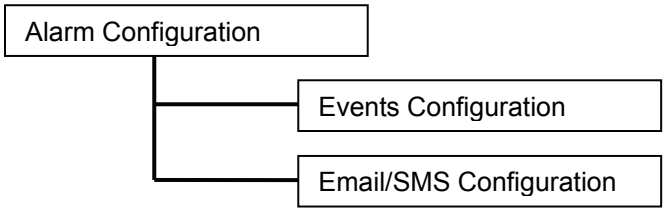
Edit:

The existing entry also can be modified after pressing **<Edit>** button.

Delete:

Remove the existing entry of allowed group configuration from the allowed group.

3-16. Alarm Configuration



Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 24 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent when users tick (☑) the trap event individually on the web page shown as below.

Parameter description:

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode Vlan Enabled, Double-tag Vlan Enabled

Module Swap: Module Inserted, Module Removed, Dual Media Swapped

3-16-1 Events

Function name:

Email/SMS Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-61). Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 24 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click **<Apply>** button to complete the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

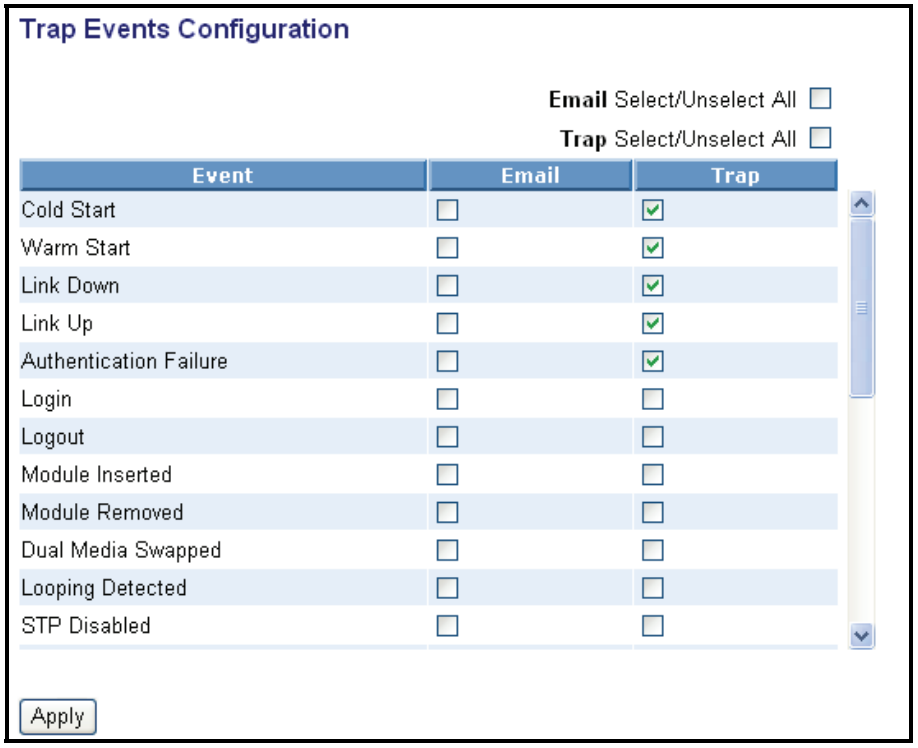


Fig. 3-165

3-16-2 Email

Parameter description:

Email:

Mail Server: the IP address of the server transferring your email.

Username: your username on the mail server.

Password: your password on the mail server.

Email Address 1 – 6: email address that would like to receive the alarm message.

SMS:

SMS Server: the IP address of the server transferring your SMS.

Username: your username in ISP.

Password: your username in ISP.

Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message.

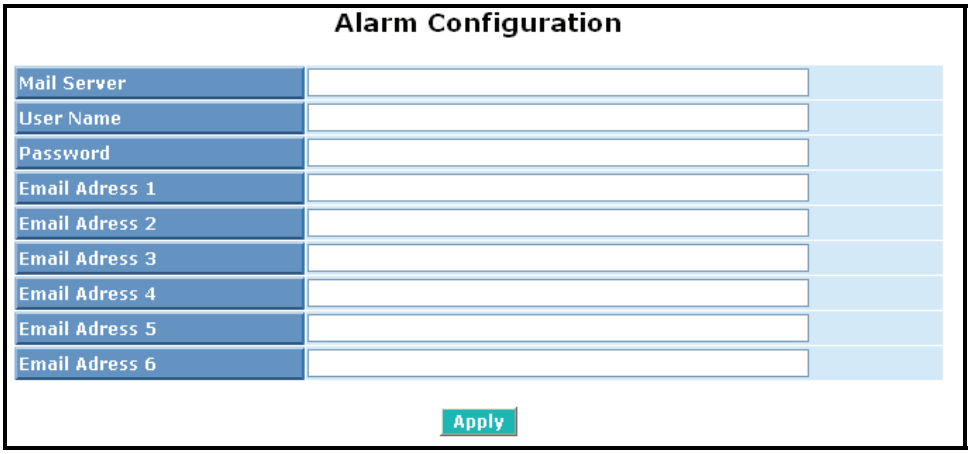


Fig. 3-166

3-17. Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

- **Default Configuration:**

This is ex-factory setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore to the default setting of the switch. One is the function of "Restore Default Configuration included default IP address", the IP address will restore to default "192.168.1.1" as you use it. The other is the function of "Restore Default Configuration without changing current IP address", the IP address will keep the same one that you had saved before by performing this function.

- **Working Configuration:**

It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you press **<Apply>** button.

- **User Configuration:**

It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.

3-17-1. Factory Defaults

Function name:

Restore Default Configuration (includes default IP address)

Function description:

Restoring Default Configuration function can retrieve factory settings to replace the start configuration and the IP address of the switch will also be restored to 192.168.1.1.

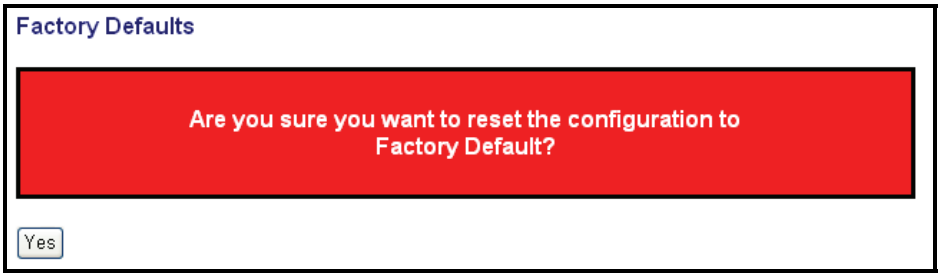


Fig. 3-167

3-17-2 . Save Start

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.

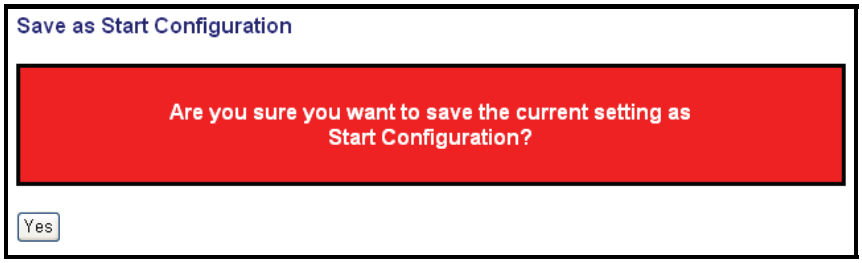


Fig. 3-168

3-17-3 . Save User

Function name:

Save As User Configuration

Function description:

Save the current configuration as a user configuration file in flash memory.

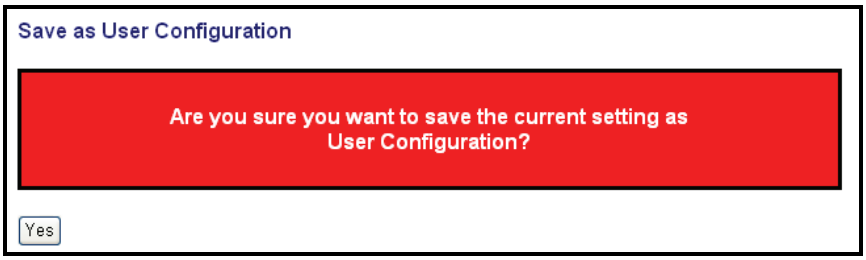


Fig. 3-169

3-17-4 . *Restore User*

Function name:

Restore User Configuration

Function description:

Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing the restore, the system's start configuration is updated and will change its system settings after rebooting the system.

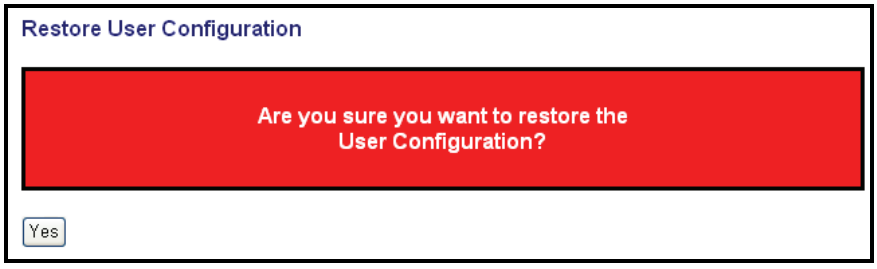


Fig. 3-170

3-18. Config File

Function name:

Config File

Function description:

With this function, user can back up or reload the configuration files of Save As Start or Save As User via TFTP.

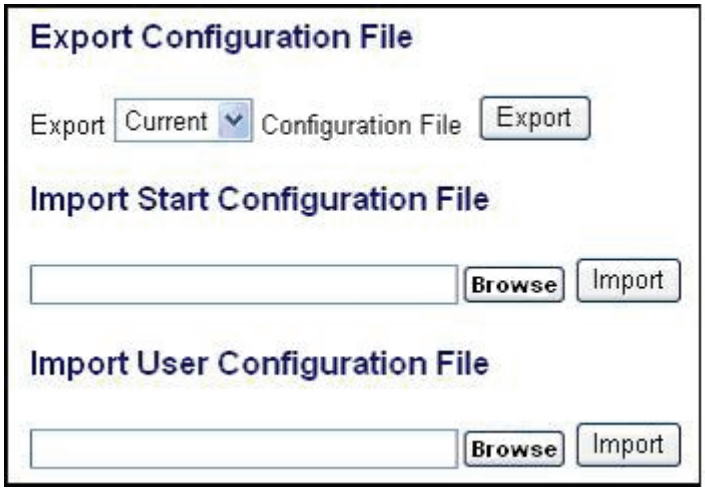


Fig. 3-171

Parameter description:

Export File Path:

Export Start:

Export Save As Start's config file stored in the flash.

Export User-Conf:

Export Save As User's config file stored in the flash.

Import File Path:

Import Start:

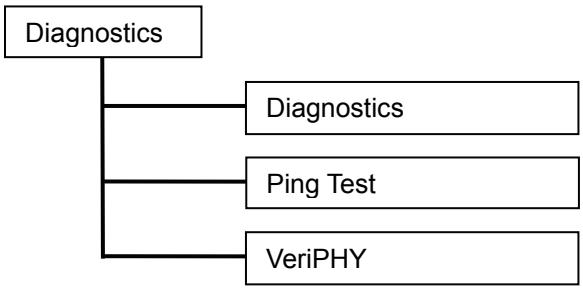
Import Save As Start's config file stored in the flash.

Import User-Conf:

Import Save As User's config file stored in the flash.

3-19. Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail in the following sections.



3-19-1 . Diagnostics

Function name:

Diagnostics

Function description:

Diagnostics function provides a set of basic system diagnosis. It allows users to know whether the system is healthy or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

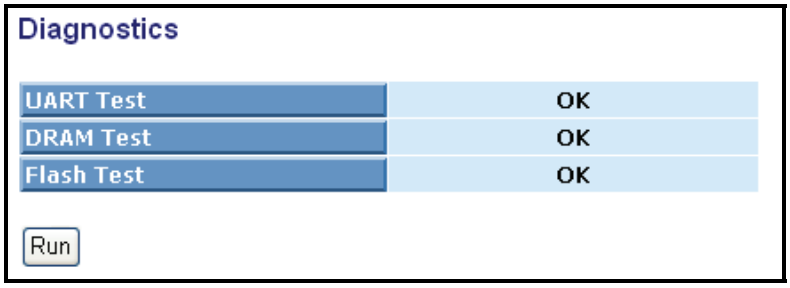


Fig. 3-172

3-19-2 .Ping

Function name:

Ping Test

Function description:

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know if the target device is available or not. You can simply fill in a known IP address and then click **<Ping>** button. After a few seconds, the switch will report if the pinged device is alive or dead in the field of Ping Result.

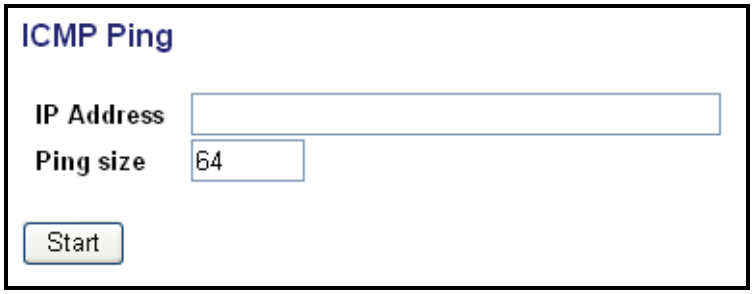


Fig. 3-173

Parameter description:

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

For more details, please see the section of IP address in Chapter 2.

3-19-2 .VeriPHY

Function name:

VeriPHY

Function description:

The switch device includes a comprehensive suite of cable diagnostic function that are available using SMI reads and writes. These functions enable a variety of cable operating conditions and status to be accessed and checked. The VeriPHY suite has the ability to identify the cable and operating conditions and to isolate a variety of common faults that can occur the Cat5 twisted pair cabling.

Note: If a link is established on the twisted pair interface in 1000BASE-T mode, VeriPHY can run without disruption of the link or disruption of any data transfer. However, if a link is established in 100Base-TX or 10Base-T, VeriPHY will cause the link to drop while the diagnostics are running. After the diagnostics are finished, the link will be re-established.

The fillowing diagnostic functions are part of the VeriPHY suite:
- Detection of coupling between cable pairs
- Detection of cable pair termination
- Determination of cable length

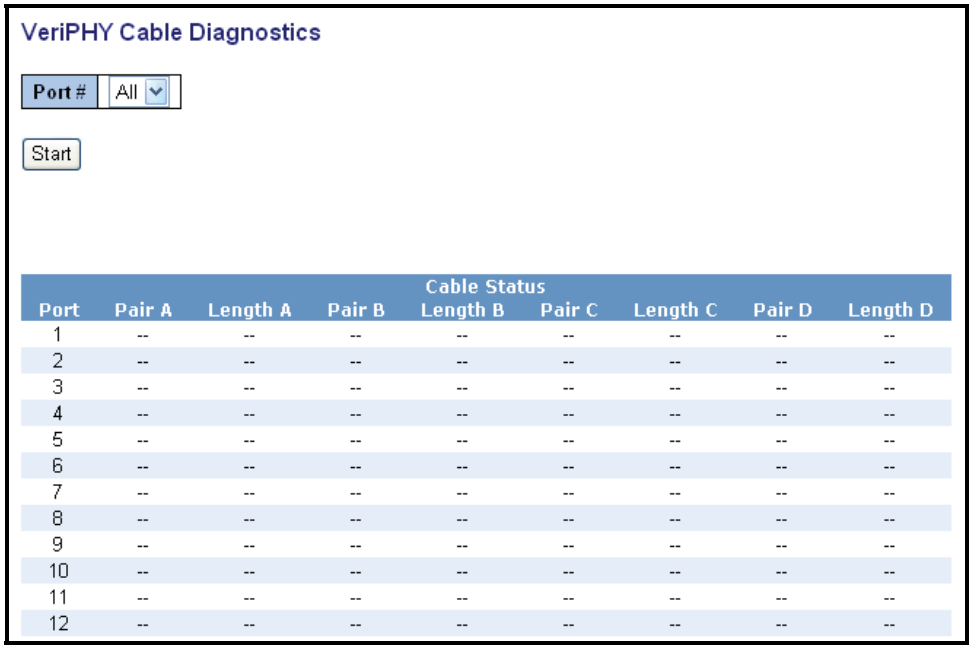

VeriPHY Cable Diagnostics
Port #
All
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- --
8 -- -- -- -- -- -- -- --
9 -- -- -- -- -- -- -- --
10 -- -- -- -- -- -- -- --
11 -- -- -- -- -- -- -- --
12 -- -- -- -- -- -- -- --

Fig. 3-174

Parameter description:

Port #: Range = 1-16 / All

You can select one port or all ports to do cable diagnostics function.

3-20 Maintenance

This chapter will introduce the reset and firmware upgrade function for the firmware upgrade and key system maintenance requirements.

3-20-1 .Reset Device

Function name:

Reset Device

Function description:

We offer you many ways to reset the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, you must reboot to have the new configuration take effect.

Fig. 3-175

3-20-2 .Software Upload

Function name:

Software Upload

Function description:

Click on <Browse> to select a specific SG71660MA firmware file from the Web management PC, then click on <Upload> to confirm the upgrade firmware action. The new firmware will be uploaded into the switch and write into flash memory. You have to reboot the switch for new firmware to take affect after upgrading the firmware.

Fig. 3-176

3-21 Logout

You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

Function name:

Logout

Function description:

The switch allows you to logout of the system to prevent other users from accessing the system without permission. If you do not logout and exit the browser, the switch will automatically have you logout in five minutes. Besides the manual logout.

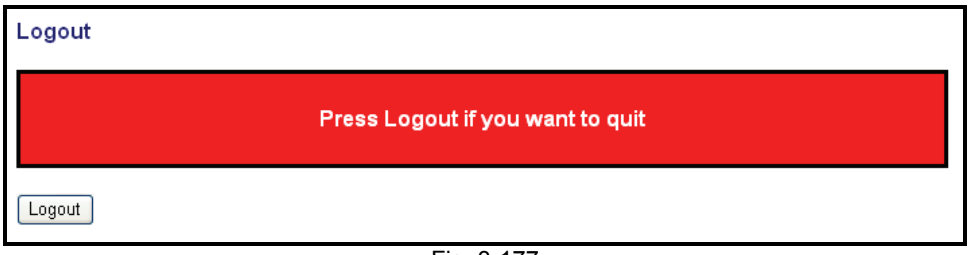


Fig. 3-177

Parameter description:

Logout:

Click on <Logout> to leave the web UI management function.

4. Operation of CLI Management

4-1. CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

-- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

-- At “Com Port Properties” Menu, configure the parameters as below: (see the next section)

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4-1-1. Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin
Password: admin

After you login successfully, the prompt will be shown as “**#**“ if you are the first login person and your authorization is administrator; otherwise it may show “**$**“. See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to change any settings for this switch.

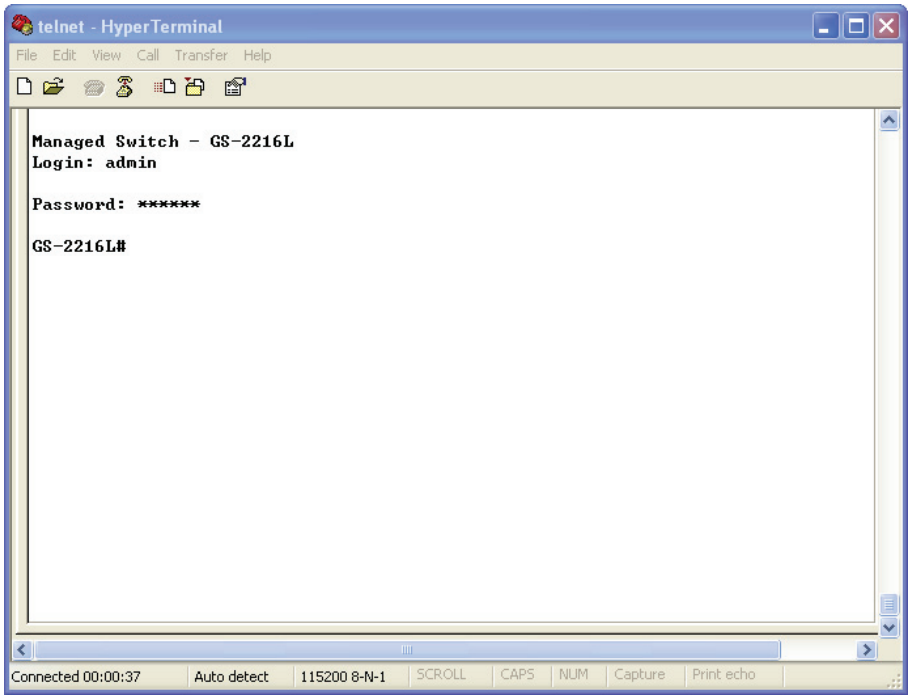

telnet - HyperTerminal
File Edit View Call Transfer Help
Managed Switch - GS-2216L
Login: admin
Password: ******
GS-2216L#
Connected 00:00:37
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Fig. 4-1

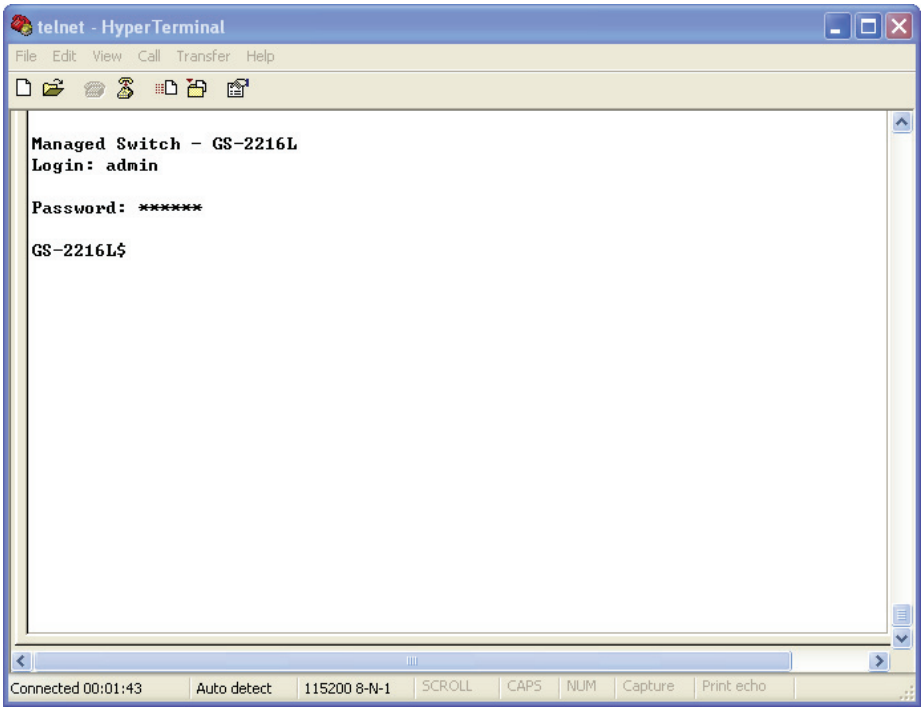

telnet - HyperTerminal
File Edit View Call Transfer Help
Managed Switch - GS-2216L
Login: admin
Password: ******
GS-2216L$
Connected 00:01:43
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Fig. 4-2

4-2. Commands of CLI

To see the commands of the mode, please input "**?**" after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. Global commands can be used regardless of the mode you are in. They are "exit", "end", "help", "history", "logout", "save start", "save user", "restore default" and "restore user". For more details, please refer to Section 4-2-1.

Command instructions residing in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different function in different modes. For example, "show" in IP mode performs displaying the IP information; however, it performs displaying the system information in system mode. For more details, please refer to Section 4-2-2.

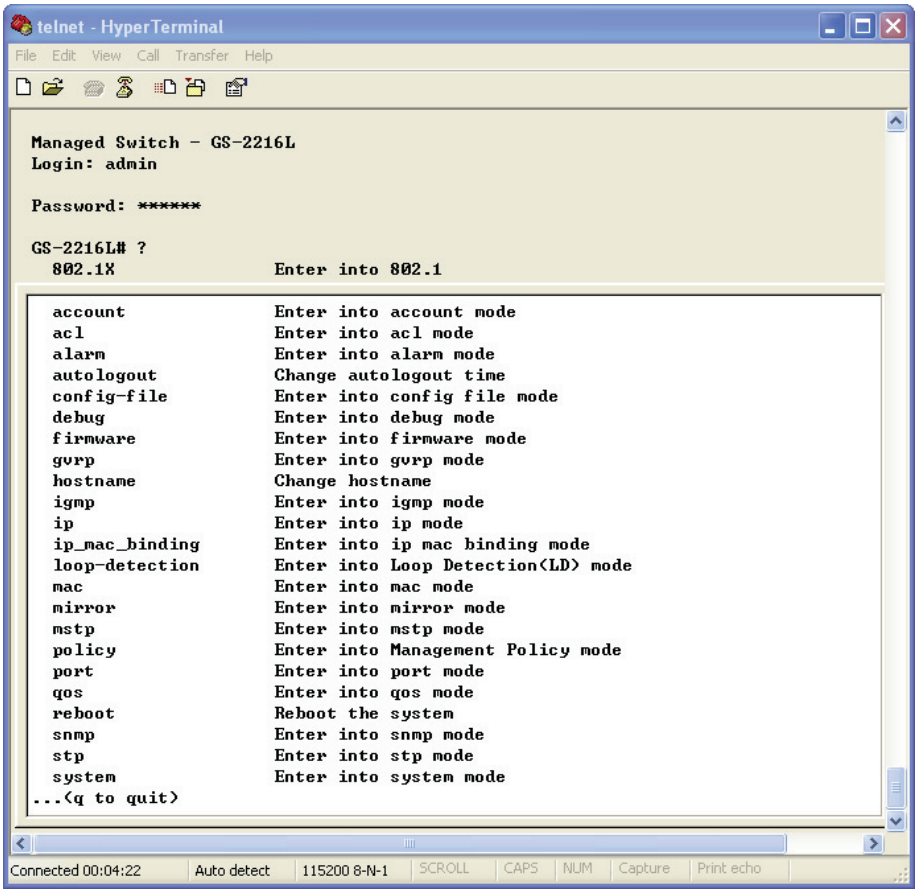


Fig. 4-3

4-2-1. Global Commands of CLI

end

Syntax:
end
Description:
Back to the top mode.
When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# alarm

GS-2216L(alarm)# events

GS-2216L(alarm-events)# end

GS-2216L#

exit

Syntax:
exit
Description:
Back to the previous mode.
When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# trunk

GS-2216L(trunk)# exit

GS-2216L#

help

Syntax:
help
Description:
To show available commands.
Some commands are the combination of more than two words. When you enter this command, the CLI shows the complete commands. The command would help you classify the commands between the local commands and the global ones.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# ip

GS-2216L(ip)# help

Commands available:

```
  ------------<< Local commands >>------------
  set ip              Set ip,subnet mask and gateway
  set dns             Set dns
  enable dhcp         Enable DHCP, and set dns auto or manual
  disable dhcp        Disable DHCP
  show                Show IP Configuration
  ------------<< Global commands >>------------
  exit                Back to the previous mode
  end                 Back to the top mode
  help                Show available commands
  history             Show a list of previously run commands
  logout              Logout the system
  save start          Save as start config
  save user           Save as user config
  restore default     Restore default config
  restore user        Restore user config
```

history

Syntax:
history [#]
Description:
To show a list of previous commands that you had previously run.
When you enter this command, the CLI shows a list of commands which you had previously typed. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.
Argument:
[#]: show last number of history records. (optional)
Possible value:
[#]: 1, 2, 3, …., 256
Example:

```
GS-2216L(ip)# history
 Command history:
  0. trunk
  1. exit
  2. GS-2216L# trunk
  3. GS-2216L(trunk)# exit
  4. GS-2216L#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
 10. end
 11. ip
 12. help
 13. ip
 14. history

GS-2216L(ip)# history 3
 Command history:
 13. ip
 14. history
 15. history 3

GS-2216L(ip)#
```

logout

Syntax:
logout
Description:
When you enter this command via Telnet connection, you would logout of the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# logout

restore default

Syntax:
restore default
Description:
When you use this function in CLI, the system will show you the information “Do you want to restore the default IP address?(y/n)”. If you choose Y or y, the IP address will restore to default “192.168.1.1”. If you choose N or n, the IP address will keep the same one that you had saved before.

If successful, the CLI would prompt if you would like to reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

Argument:
None.
Possible value:
None.
Example:

GS-2216L# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.

restore user

Syntax:
restore user
Description:
To restore the startup configuration as user defined configuration. If successful, the CLI would prompt if you would like to reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise would be back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would be replaced as user defined one.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# restore user

Restoring ...

Restore User Configuration Successfully

Press any key to reboot system.

save start

Syntax:
save start
Description:
To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration to work after rebooting, save the configuration using the command ‘save start’.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# save start

Saving start...

Save Successfully

GS-2216L#

save user

Syntax:
save user
Description:
To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# save user

Saving user...

Save Successfully

GS-2216L#

4-2-2. Local Commands of CLI

■ 802.1X

set max-request

Syntax:
set max-request <port-range> <times>
Description:
The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<times>: max-times , range 1-10
Possible value:
<port range> : 1 to 16
<times>: 1-10, default is 2
Example:

GS-2216L(802.1X)# set max-request 2 2

set mode

Syntax:
set mode <port-range> <mode>
Description:
To set up the 802.1X authentication mode of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<mode>: set up 802.1X mode
0:disable the 802.1X function
1:set 802.1X to Multi-host mode
Possible value:
<port range> : 1 to 16
<mode>: 0 or 1
Example:

GS-2216L(802.1X)# set mode 2 1

GS-2216L(802.1X)#

set port-control

Syntax:
set port-control <port-range> <authorized>
Description:
To set up 802.1X status of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<authorized> : Set up the status of each port
0:ForceUnauthorized
1:ForceAuthorized
2:Auto
Possible value:
<port range> : 1 to 16
<authorized> : 0, 1 or 2
Example:

GS-2216L(802.1X)# set port-control 2 2

set quiet-period

Syntax:
set quiet-period <port-range> <sec>
Description:
A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<sec> : timer , range 0-65535
Possible value:
<port range> : 1 to 16
<sec> : 0-65535, default is 60
Example:

GS-2216L(802.1X)# set quiet-period 2 30

set reAuthEnabled

Syntax:
set reAuthEnabled <port-range> <ebl>
Description:
A constant that defines whether regular reauthentication will take place on this port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<ebl> :
0:OFF Disable reauthentication
1:ON Enable reauthentication
Possible value:
<port range> : 1 to 16
<ebl> : 0 or 1, default is 1
Example:

GS-2216L(802.1X)# set reAuthEnabled 2 1

set reAuthMax

Syntax:
set reAuthMax <port-range> <max>

Description:
The number of reauthentication attempts that are permitted before the port becomes Unauthorized.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<max> : max. value , range 1-10
Possible value:
<port range> : 1 to 16
<max> : 1-10, default is 2
Example:

GS-2216L(802.1X)# set reAuthMax 2 2

set reAuthPeriod

Syntax:
set reAuthPeriod <port-range> <sec>
Description:
A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 16
<sec> : 1-65535, default is 3600
Example:

GS-2216L(802.1X)# set reAuthPeriod 2 3600

set serverTimeout

Syntax:
set serverTimeout <port-range> <sec>
Description:
A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 16
<sec> : 1-65535, default is 30
Example:

GS-2216L(802.1X)# set serverTimeout 2 30

set state

Syntax:
set state <ip> <port-number> <secret-key>
Description:
To configure the settings related with 802.1X Radius Server.
Argument:
<ip> : the IP address of Radius Server
<port-number> : the service port of Radius Server(Authorization port)
<secret-key> : set up the value of secret-key, and the length of secret-key is from 1 to 31
Possible value:
<port-number> : 1~65535, default is 1812
Example:

GS-2216L(802.1X)# set state 192.168.1.115 1812 WinRadius

set suppTimeout

Syntax:
set suppTimeout <port-range> <sec>
Description:
A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 16
<sec> : 1-65535, default is 30
Example:

GS-2216L(802.1X)# set suppTimeout 2 30

set txPeriod

Syntax:
set txPeriod <port-range> <sec>
Description:
A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted
Argument:
<port range> : syntax 1,5-7, available from 1 to 16
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 16
<sec> : 1-65535, default is 30
Example:

GS-2216L(802.1X)# set txPeriod 2 30

show mode

Syntax:
show mode
Description:

To display the mode of each port.
Argument:
None
Possible value:
None
Example:

```
GS-2216L(802.1X)# show mode
 Port      Mode
====== ============
   1     Disable
   2     Multi-host
   3     Disable
   4     Disable
   5     Disable
   6     Disable
           :
           :
           :
```

show parameter

Syntax:
show parameter
Description:
To display the parameter settings of each port.
Argument:
None
Possible value:
None
Example:

```
GS-2216L(802.1X)# show parameter
port  1) port control  : Auto
        reAuthMax     : 2
        txPeriod      : 30
        Quiet Period  : 60
        reAuthEnabled : ON
        reAuthPeriod  : 3600
        max. Request  : 2
        suppTimeout   : 30
        serverTimeout : 30
```

port 2) port control : Auto

reAuthMax : 2

txPeriod : 30

Quiet Period : 60

reAuthEnabled : ON

reAuthPeriod : 3600

max. Request : 2

suppTimeout : 30

serverTimeout : 30

:

:

:

show security

Syntax:
show security
Description:
To display the authentication status of each port.
Argument:
None
Possible value:
None
Example:

GS-2216L(802.1X)# show security

Port	Mode	Status
1	Disable	
2	Multi-host	Unauthorized
3	Disable	
4	Disable	
5	Disable	
6	Disable	
:		
:		

show state

Syntax:
show state
Description:
Show the Radius server configuration
Argument:
None
Possible value:
None
Example:

GS-2216L(802.1X)# show state

Radius Server: 192.168.1.115

Port Number : 1812

Secret Key : WinRadius

■ acl

ace

Syntax:
ace <index>
Description:
To display the ace configuration.
Argument:
<index> : the access control rule index value
Possible value:
None.
Example:
GS-2216L(acl)# ace 2

index: 2

rule: switch

vid: any

tag_prio: any

dmac: any

frame type: arp

arp type: Request/Reply (opcode): any

source ip: any

destination ip: any

ARP flag

ARP SMAC Match: any

RARP DMAC Match: any

IP/Ethernet Length: any

IP: any

Ethernet: any

action: 1

rate limiter: 0

copy port: 0

action

Syntax:
action <port> <permit|deny> <rate_limiter> <port copy>
Description:
To set the access control per port as packet filter action rule.
Argument:
<port> : 1-24
<permit/deny>: permit: 1, deny: 0

<rate_limiter>: 0-16 (0:disable)
<port copy> : 0-24 (0:disable)
Possible value:
<port> : 1-24
<permit/deny>: 0-1
<rate_limiter>: 0-16
<port copy> : 0-24
Example:

```
GS-2216L(acl)# action 5 0 2 2

GS-2216L(acl)# show

port policy id  action   rate limiter port copy   counter a class map

 ..      ..    …….    ….         …             ..

 5       1     deny      2         2

 23      1    permit     0         0             0

 24      1    permit     0         0             0


rate limiter   rate(pps)

------------ ------------

     1              1

     2              1

     3              1

     4              1

     5              1


     ……          ……

GS-2216L(acl)#
```

delete

Syntax:
delete <index>
Description:
To delete the ACE (Access Control Entry) configuration on the switch.
Argument:
<index> : the access control rule index value
Possible value:
None.
Example:

```
GS-2216L(acl)# delete 1

GS-2216L(acl)#
```

move

Syntax:
move <index1> <index2>
Description:
To move the ACE (Access Control Entry) configuration between index1 and index2..
Argument:

None.
Possible value:
None.
Example:

```
GS-2216L(account)# move 1 2
```

policy

Syntax:
policy <policy> <ports>
Description:
To set acl port policy on switch
Argument:
<policy> : 1-8
<ports> : 1-24
Possible value:
<policy> : 1-8
<ports> : 1-24
Example:

```
GS-2216L(acl)# policy 3 10

GS-2216L(acl)#
```

ratelimiter

Syntax:
ratelimiter <id> <rate>
Description:
To set access control rule with rate limiter on switch
Argument:
<id> : 1-16
<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,
16000,32000,64000,128000,256000,512000,1024000
Possible value:
<id> : 1-16
<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,
16000,32000,64000,128000,256000,512000,1024000
Example:

```
GS-2216L(acl)# ratelimiter 3 16000

GS-2216L(acl)#
```

set

Syntax:

```
set [<index>] [<next index>]
        [switch | (port <port>) | (policy <policy>)]
        [<vid>] [<tag_prio>] [<dmac_type>]
        [(any) |
         (etype [<etype>] [<smac>]) |
         (arp [<arp type>] [<opcode>]
             (any | [<source ip>] [<source ip mask>])
             (any | [<destination ip>] [<destination ip mask>])
```

[<source mac>] [<arp smac match flag>]
[<raro dmac match flag>] [<ip/ethernet length flag>]
[<ip flag>] [<ethernet flag>]) |
(ip [(<source ip> <source ip mask>) | any]
[(<destination ip> <destination ip mask>) | any]
[<ip ttl>] [<ip fragment>] [<ip option>]
[(icmp <icmp type> <icmp code>) |
(udp <source port range> <destination port range>) |
(tcp <source port range> <destination port range>
<tcp fin flag> <tcp syn flag> <tcp rst flag>
<tcp psh flag> <tcp ack flag> <tcp urg flag>) |
(other <ip protocol value>) |
(any)]
]
[<action>] [<rate limiter>] [<port copy>]

Description:
To set access control entry on switch
Argument:

Possible value:

Example:

show

Syntax:
show
Description:
To show all access control entry setting on switch
Argument:
none
Possible value:
none
Example:

GS-2216L(acl)# show

port policy id action rate limiter port copy counter a class map

.. .. ……. …. … ..

5 1 deny 2 2

23 1 permit 0 0 0

24 1 permit 0 0 0

rate limiter rate(pps)

---------- ----------

1 1

2 1

3 1

4 1

5 1

…… ……

GS-2216L(acl)#

■ account

add

Syntax:
add <name>
Description:
To create a new guest user. When you create a new guest user, you must type in password and confirm password.
Argument:
<name> : new account name
Possible value:
A string must be at least 5 character.
Example:

GS-2216L(account)# add aaaaa

Password:

Confirm Password:

Save Successfully

GS-2216L(account)#

del

Syntax:
del <name>
Description:
To delete an existing account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

GS-2216L(account)# del aaaaa

Account aaaaa deleted

modify

Syntax:
modify <name>
Description:
To change the username and password of an existing account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

GS-2216L(account)# modify aaaaa

username/password: the length is from 5 to 15.

Current username (aaaaa):bbbbb

New password:

Confirm password:

Username changed successfully.

Password changed successfully.

show

Syntax:
show
Description:
To show system account, including account name and identity.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(account)# show

Account Name Identity

---------- ----------

admin Administrator

guest guest

■ alarm

<<email>>

del mail-address

Syntax:
del mail-address <#>
Description:
To remove the configuration of E-mail address.
Argument:
<#>: email address number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:

GS-2216L(alarm-email)# del mail-address 2

del server-user

Syntax:
del server-user
Description:
To remove the configuration of server, user account and password.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(alarm-email)# del server-user

set mail-address

Syntax:
set mail-address <#> <mail address>
Description:
To set up the email address.
Argument:
<#> :email address number, range: 1 to 6
<mail address>:email address
Possible value:
<#>: 1 to 6
Example:

GS-2216L(alarm-email)# set mail-address 1 abc@mail.abc.com

set server

Syntax:
set server <ip>
Description:
To set up the IP address of the email server.
Argument:
<ip>:email server ip address or domain name
Possible value:
None.
Example:

GS-2216L(alarm-email)# set server 192.168.1.6

set user

Syntax:
set user <username>
Description:
To set up the account and password of the email server.
Argument:
<username>: email server account and password
Possible value:
None.
Example:

GS-2216L (alarm-email)# set user admin

show

Syntax:
show
Description:
To display the configuration of e-mail.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(alarm-email)# show

Mail Server : 192.168.1.6

Username : admin

Password : **********

Email Address 1: abc@mail.abc.com

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

<<events>>

del all

Syntax:
del all <range>
Description:
To disable email, sms and trap of events.
Argument:
<range>:del the range of events, syntax 1,5-7
Possible value:
<range>: 1~16
Example:

GS-2216L(alarm-events)# del all 1-3

del email

Syntax:
del email <range>
Description:
To disable the email of the events.
Argument:
<range>:del the range of email, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

GS-2216L(alarm-events)# del email 1-3

del sms

Syntax:
del sms <range>
Description:
To disable the sms of the events.
Argument:
<range>:del the range of sms, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

GS-2216L(alarm-events)# del sms 1-3

del trap

Syntax:
del trap <range>
Description:
To disable the trap of the events.
Argument:
<range>:del the range of trap, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

GS-2216L(alarm-events)# del trap 1-3

set all

Syntax:
set all <range>
Description:
To enable email, sms and trap of events.
Argument:
<range>:set the range of events, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

GS-2216L(alarm-events)# set all 1-3

set email

Syntax:
set email <range>
Description:
To enable the email of the events.
Argument:
<range>:set the range of email, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

GS-2216L(alarm-events)# set email 1-3

set sms

Syntax:
set sms <range>
Description:
To enable the sms of the events.
Argument:
<range>:set the range of sms, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

```
GS-2216L(alarm-events)# set sms 1-3
```

set trap

Syntax:
set trap <range>
Description:
To enable the trap of the events.
Argument:
<range>:set the range of trap, syntax 1,5-7
Possible value:
<range>: 1~24
Example:

```
GS-2216L(alarm-events)# set trap 1-3
```

show

Syntax:
show
Description:
To display the configuration of alarm event.
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(alarm-events)# show
  Events                Email SMS Trap
----------------------------------------
1  Cold Start                  v
2  Warm Start                    v
3  Link Down                     v
4  Link Up                     v
5  Authentication Failure          v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
```

11 LACP Disabled

12 LACP Enabled

13 LACP Member Added

14 LACP Port Failure

15 GVRP Disabled

16 GVRP Enabled

17 VLAN Disabled

18 Port-based Vlan Enabled

19 Tag-based Vlan Enabled

20 Metro-mode Vlan Enabled

21 Double-tag Vlan Enabled

22 Module Inserted

23 Module Removed

24 Moudle Media Swapped

show (alarm)

Syntax:
show
Description:
The Show for alarm here is used to display the configuration of Trap, SMS or E-mail.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(alarm)# show events

GS-2216L(alarm)# show email

GS-2216L(alarm)# show sms

<<sms>>

del phone-number

Syntax:
del phone-number <#>
Description:
To delete sms phone number.
Argument:
<#>: mobile phone number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:

GS-2216L(alarm-sms)# del phone-number 3

del server-user

Syntax:

del server-user
Description:
To delete sms server, user account and password.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(alarm-sms)# del server-user

set phone-number

Syntax:
set phone-number <#> <phone-number>
Description:
To add sms phone number.
Argument:
<#>: mobile phone number, range: 1 to 6
<phone-number>: phone number
Possible value:
<#>: 1 to 6
Example:

GS-2216L(alarm-sms)# set phone-number 1 0968777777

set server

Syntax:
set server <ip>
Description:
To set up the IP address of sms server.
Argument:
<ip>: SMS server ip address or domain name
Possible value:
None.
Example:

GS-2216L(alarm-sms)# set server 192.168.1.7

set user

Syntax:
set user <username>
Description:
To set up user account and password of sms server.
Argument:
<username>: SMS server account
Possible value:
None.
Example:

GS-2216L(alarm-sms)# set user ABC

show

Syntax:
show
Description:
To display the configuration of SMS trap event.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(alarm-sms)# show

SMS Server : 192.168.1.7

Username : ABC

Password : **********

Mobile Phone 1: 0968777777

Mobile Phone 2:

Mobile Phone 3:

Mobile Phone 4:

Mobile Phone 5:

Mobile Phone 6:

■ autologout

autologout

Syntax:
autologout <time>
Description:
To set up the timer of autologout.
Argument:
<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
Possible value:
<time>: 0,1-3600
Example:

GS-2216L# autologout 3600

Set autologout time to 3600 seconds

■ bandwidth

disable egress-rate

Syntax:
disable egress-rate <range>
Description:
To cancel the egress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(bandwidth)# disable egress-rate 1-8

disable ingress-rate

Syntax:
disable ingress-rate <range>
Description:
To cancel the Ingress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(bandwidth)# disable ingress-rate 1-8

disable storm-rate

Syntax:
disable storm-rate <range>
Description:
To cancel the storm-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(bandwidth)# disable storm-rate 1-8

enable egress-rate

Syntax:
enable egress-rate <range> <data_rate>
Description:
To set up the egress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
<data_rate>: 0-1000
Possible value:
<range>: 1 to 16
<data_rate>: 0-1000
Example:

GS-2216L(bandwidth)# enable egress-rate 1-16 200

enable ingress-rate

Syntax:
enable ingress-rate <range> <data_rate>
Description:
To set up the Ingress-rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
<data_rate>: 0-1000
Possible value:
<range>: 1 to 16
<data_rate>: 0-1000
Example:

GS-2216L(bandwidth)# enable ingress-rate 1-16 100

enable storm-rate

Syntax:
enable storm-rate <range> <data_rate>
Description:
To set up the storm-rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
<data_rate>: 0-1000
Possible value:
<range>: 1 to 16
<data_rate>: 0-1000
Example:

GS-2216L(bandwidth)# enable strom-rate 1-16 150

show

Syntax:
show

Description:
To display all current settings of the bandwidth.
Argument:
None
Possible value:
None
Example:

GS-2216L(bandwidth)# show

Port	Ingress				Egress	
	All State	All Rate	Storm State	Storm Rate	All state	All Rate
1	Disabled	0	Disabled	0	Disabled	0
2	Disabled	0	Disabled	0	Disabled	0
3	Disabled	0	Disabled	0	Disabled	0
4	Disabled	0	Disabled	0	Disabled	0
5	Disabled	0	Disabled	0	Disabled	0
6	Disabled	0	Disabled	0	Disabled	0
7	Disabled	0	Disabled	0	Disabled	0
8	Disabled	0	Disabled	0	Disabled	0
9	Disabled	0	Disabled	0	Disabled	0
10	Disabled	0	Disabled	0	Disabled	0
11	Disabled	0	Disabled	0	Disabled	0
12	Disabled	0	Disabled	0	Disabled	0
13	Disabled	0	Disabled	0	Disabled	0
14	Disabled	0	Disabled	0	Disabled	0
15	Disabled	0	Disabled	0	Disabled	0
16	Disabled	0	Disabled	0	Disabled	0
17	Disabled	0	Disabled	0	Disabled	0
18	Disabled	0	Disabled	0	Disabled	0
19	Disabled	0	Disabled	0	Disabled	0
20	Disabled	0	Disabled	0	Disabled	0

...(q to quit)

21	Disabled	0	Disabled	0	Disabled	0
22	Disabled	0	Disabled	0	Disabled	0
23	Disabled	0	Disabled	0	Disabled	0
16	Disabled	0	Disabled	0	Disabled	0

■ config-file

export start

Syntax:
export start
Description:
To run the export start function.
Argument:
None
Possible value:
None
Example:

GS-2216L(config-file)# export start

Export successful.

export user-conf

Syntax:
export user-conf
Description:
To run the export user-conf function.
Argument:
None
Possible value:
None
Example:

GS-2216L(config-file)# export user-conf

Export successful.

import start

Syntax:
import start
Description:
To run the import start function.
Argument:
None
Possible value:
None
Example:

GS-2216L(config-file)# import start

Import successful.

import user-conf

Syntax:
import user-conf
Description:
To run the import user-conf function.
Argument:
None
Possible value:
None
Example:

GS-2216L(config-file)# import user-conf

Import successful.

set export-path

Syntax:
set export-path <filepath>
Description:
To set up the filepath and filename that will be exported.
Argument:
<filepath>:filepath and filename
Possible value:
<filepath>:filepath and filename
Example:

GS-2216L(config-file)# set export-path log/21511.txt

set import-path

Syntax:
set import-path <filepath>
Description:
To set up the filepath and filename that will be imported.
Argument:
<filepath>:filepath and filename
Possible value:
<filepath>:filepath and filename
Example:

GS-2216L(config-file)# set import-path log/21511.txt

show

Syntax:
show
Description:
To display the config-file information.
Argument:
None
Possible value:
None
Example:

GS-2216L(config-file)# show

TFTP Server IP Address: 192.168.3.111

Export Path and Filename: nmap/123.ts

Import Path and Filename: user123.txt

■ dhcp-boot

set dhcp-boot

Syntax:
set dhcp-boot <sec>
Description:
To set up the delay time for DHCP Boot.
Argument:
<sec>:range syntax: 0, 1-30. The value “0” is to disable dhcp-boot delay
Possible value:
<sec>:0-30
Example:

GS-2216L(dhcp-boot)# set dhcp-boot 30

show

Syntax:
show
Description:
To display the status of DHCP Boot.
Argument:
None
Possible value:
None
Example:

GS-2216L(dhcp-boot)#show

dhcp boot : Enable

Second : 10

■ diag

diag

Syntax:
diag
Description:
Diag is used to test whether UART, DRAM, Flash and EEPROM is normal or not.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(diag)# diag

EEPROM Test : OK

UART Test : OK

DRAM Test : OK

Flash Test : OK

loopback

Syntax:
Loopback
Description:
For Internal/External Loopback Test.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(diag)# loopback

Internal Loopback Test : OK

External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 Fail

ping

Syntax:
ping <ip>
Description:
To confirm that whether the remote end-station or switch itself is alive or not.
Argument:
<ip> : ip address or domain name
Possible value:
IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com
Example:

GS-2216L(diag)# ping 192.168.1.115

Gateway : 192.168.1.253

192.168.1.115 is alive.

■ firmware

set upgrade-path

Syntax:
set upgrade-path <filepath>
Description:
To set up the image file that will be upgraded.
Argument:
<filepath>: upgrade file path
Possible value:
<filepath>: upgrade file path
Example:

GS-2216L(firmware)# set upgrade-path GEL2P-SW24_GS-2216L_v2.03.img

show

Syntax:
show
Description:
To display the information of tftp server and upgrade-path.
Argument:
None
Possible value:
None
Example:

GS-2216L(firmware)# show

TFTP Server IP Address: 192.168.3.111

Path and Filename : GEL2P-SW24_GS-2216L_v2.03.img

upgrade

Syntax:
upgrade
Description:
To run the upgrade function.
Argument:
None
Possible value:
None
Example:

GS-2216L(firmware)# upgrade

Upgrading firmware ...

■ gvrp

disable

Syntax:
disable
Description:
To disable the gvrp function.
Argument:
None
Possible value:
None
Example:

GS-2216L(gvrp)# disable

enable

Syntax:
enable
Description:
To enable the gvrp function.
Argument:
None
Possible value:
None
Example:

GS-2216L(gvrp)# enable

group

Syntax:
group <group number>
Description:
To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.
Argument:
<group number>: enter which gvrp group you had created, using value is vid. Available range: 1 to 4094
Possible value:
<group number>: 1~4094
Example:

GS-2216L(gvrp)# show group

GVRP group information

Current Dynamic Group Number: 1

VID Member Port

---- --

2 5

```
GS-2216L(gvrp)# group 2
GS-2216L(gvrp-group-2)# set applicant 1-6 non-participant

GS-2216L(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Normal
2    Non-Participant Normal
3    Non-Participant Normal
4    Non-Participant Normal
5    Non-Participant Normal
6    Non-Participant Normal
7    Normal          Normal
8    Normal          Normal
12   Normal          Normal
13   Normal          Normal
                     :
                     :
23   Normal          Normal
24   Normal          Normal

GS-2216L(gvrp-group-2)# set registrar 1-10 fixed

GS-2216L(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Fixed
2    Non-Participant Fixed
3    Non-Participant Fixed
4    Non-Participant Fixed
5    Non-Participant Fixed
6    Non-Participant Fixed
7    Normal          Fixed
8    Normal          Fixed
9    Normal          Fixed
10   Normal          Fixed
17   Normal          Normal
               :
```

:

23	Normal	Normal
24	Normal	Normal

set applicant

Syntax:
set applicant <range> <normal|non-participant>
Description:
To set default applicant mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 16
<normal>: set applicant as normal mode
<non-participant>: set applicant as non-participant mode
Possible value:
<range>: 1 to 16
<normal|non-participant>: normal or non-participant
Example:

GS-2216L(gvrp)# set applicant 1-10 non-participant

set registrar

Syntax:
set registrar <range> <normal|fixed|forbidden>
Description:
To set default registrar mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 16
<normal>: set registrar as normal mode
<fixed>: set registrar as fixed mode
<forbidden>: set registrar as forbidden mode
Possible value:
<range>: 1 to 16
<normal|fixed|forbidden>: normal or fixed or forbidden
Example:

GS-2216L(gvrp)# set registrar 1-5 fixed

set restricted

Syntax:
set restricted <range> <enable|disable>
Description:
To set the restricted mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 16
<enable>: set restricted enabled
<disable>: set restricted disabled
Possible value:
<range>: 1 to 16
<enable|disable>: enable or disable
Example:

GS-2216L(gvrp)# set restricted 1-10 enable

GS-2216L(gvrp)# show config

GVRP state: Enable

Port	Join Time	Leave Time	LeaveAll Time	Applicant	Registrar	Restricted
1	20	60	1000	Normal	Normal	Enable
2	20	60	1000	Normal	Normal	Enable
3	20	60	1000	Normal	Normal	Enable
4	20	60	1000	Normal	Normal	Enable
5	20	60	1000	Normal	Normal	Enable
6	20	60	1000	Normal	Normal	Enable
7	20	60	1000	Normal	Normal	Enable
8	20	60	1000	Normal	Normal	Enable
9	20	60	1000	Normal	Normal	Enable
10	20	60	1000	Normal	Normal	Enable
			:		:	

set timer

Syntax:
set timer <range> <join> <leave> <leaveall>
Description:
To set gvrp join time, leave time, and leaveall time for each port.
Argument:
<range> : port range, syntax 1,5-7, available from 1 to 16
<join>: join timer, available from 20 to 100
<leave>: leave timer, available from 60 to 300
<leaveall>: leaveall timer, available from 1000 to 5000
Leave Time must equal double Join Time at least.
Possible value:
<range> : 1 to 16
<join>: 20 to 100
<leave>: 60 to 300
<leaveall>: 1000 to 5000
Example:

```
GS-2216L(gvrp)# set timer 2-8 25 80 2000
```

show config

Syntax:
show config
Description:
To display the gvrp configuration.
Argument:
None
Possible value:
None
Example:

```
GS-2216L(gvrp)# show config

GVRP state: Enable

Port Join Time Leave Time LeaveAll Time    Applicant    Registrar Restricted
---- --------- ---------- ------------- --------------- --------- ----------
  1     20         60         1000        Normal         Normal     Disable
  2     25         80         2000        Normal         Normal     Disable
  3     25         80         2000        Normal         Normal     Disable
  4     25         80         2000        Normal         Normal     Disable
  5     25         80         2000        Normal         Normal     Disable
  6     25         80         2000        Normal         Normal     Disable
  7     25         80         2000        Normal         Normal     Disable
  8     25         80         2000        Normal         Normal     Disable
                                :
                                :
```

show counter

Syntax:
show counter <port>
Description:
To display the counter number of the port.
Argument:
<port>: port number
Possible value:
<port>: available from 1 to 16
Example:

```
GS-2216L(gvrp)# show counter 2

GVRP Counter port: 2

Counter Name          Received Transmitted

--------------------  -------- -----------

Total GVRP Packets          0          0

Invalid GVRP Packets        0       ----

LeaveAll message            0          0

JoinEmpty message           0          0

JoinIn message              0          0

LeaveEmpty message          0          0

Empty message               0          0
```

show group

Syntax:
show group
Description:
To show the gvrp group.
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(gvrp)# show group

GVRP group information

VID  Member Port

---- -------------------------------------------------
```

■ hostname

hostname

Syntax:
hostname <name>
Description:
To set up the hostname of the switch.
Argument:
<name>: hostname, max. 40 characters.
Possible value:
<name>: hostname, max. 40 characters.
Example:

GS-2216L# hostname Company

Company#

■ igmp-snooping

add allowed-group

Syntax:
add allowed-group <ip-multicast> <vid> <port-range>
Description:
To add the entry of allowed IP multicast group.
Argument:
<ip-multicast>: the range of IP multicast.
<vid>: vlan ID. 0-4094 or any. “0” value means tag-based vlan disable
<port-range>: syntax 1,5-7, available from 1 to 16
Possible value:
<ip-multicast>: ex: 224.1.1.1-225.2.3.3 or any
<vid>: 0-4094 or any
<port-range>: 1 to 16
Example:

GS-2216L(igmp-snooping)# add allowed-group 224.1.1.1-225.2.3.3 100 1-10

del allowed-group

Syntax:
del allowed-group <index>
Description:
To remove the entry of allowed ip multicast group
Argument:
<index>: the index of the allowed-group.
Possible value:
<index>: the index of the allowed-group.
Example:

GS-2216L(igmp-snooping)# del allowed-group 1

set mode

Syntax:
set mode <status>
Description:
To set up the mode of IGMP Snooping.
Argument:
<status>: 0:disable, 1:active, 2:passive
Possible value:
<status>: 0,1or 2
Example:

GS-2216L(igmp-snooping)# set mode 2

show igmp-snooping

Syntax:
show igmp-snooping
Description:
To display IGMP snooping mode and allowed IP multicast entry.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(igmp-snooping)# show igmp-snooping

Snoop Mode: Active

IP Multicast:

1) IP Address : 224.1.1.1
   VLAN ID : 0
   Member Port : 22

show multicast

Syntax:
show multicast
Description:
To display IP multicast table.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(igmp-snooping)# show multicast

IP Multicast: None

■ **IP**

disable dhcp

Syntax:
disable dhcp
Description:
To disable the DHCP function of the system.
Argument:
None
Possible value:
None
Example:
GS-2216L(ip)# disable dhcp

enable dhcp

Syntax:
enable dhcp <manual|auto>
Description:
To enable the system DHCP function and set DNS server via manual or auto mode.
Argument:
<manual|auto> : set dhcp by using manual or auto mode.
Possible value:
<manual|auto> : manual or auto
Example:
GS-2216L(ip)# enable dhcp manual

set dns

Syntax:
set dns <ip>
Description:
To set the IP address of DNS server.
Argument:
<ip> : dns ip address
Possible value:
168.95.1.1
Example:
GS-2216L (ip)# set dns 168.95.1.1

set ip

Syntax:
set ip <ip> <mask> <gateway>
Description:
To set the system IP address, subnet mask and gateway.
Argument:
<ip> : ip address
<mask> : subnet mask
<gateway> : default gateway
Possible value:
<ip> : 192.168.1.2 or others
<mask> : 255.255.255.0 or others
<gateway> : 192.168.1.253 or others
Example:
GS-2216L(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

show

Syntax:
show
Description:
To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.
Argument:
None
Possible value:
None
Example:

GS-2216L(ip)# show

DHCP : Disable

IP Address : 192.168.2.237

Current IP Address : 192.168.2.237

Subnet mask : 255.255.255.0

Gateway : 192.168.2.252

DNS Setting : Manual

DNS Server : 168.95.1.1

■ log

clear

Syntax:
clear
Description:
To clear the log data.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(log)# clear

disable auto-upload

Syntax:
disable auto-upload
Description:
To disable the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(log)# disable auto-upload

enable auto-upload

Syntax:
enable auto-upload
Description:
To enable the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(log)# enable auto-upload

show

Syntax:
show
Description:
To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(log)# show


Tftp Server : 0.0.0.0

Auto Upload : Disable


1)  Wed Apr 13 12:13:27 2005  Link Up [Port 1]

2)  Wed Apr 13 12:13:26 2005  Link Down [Port 1]

3)  Wed Apr 13 11:58:31 2005  Login [admin]

4)  Wed Apr 13 11:19:45 2005  Login [admin]

5)  Wed Apr 13 11:19:37 2005  Logout [admin]
```

upload

Syntax:
upload
Description:
To upload log data through tftp.
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(log)# upload
```

■ ip_mac_binding

set entry

Syntax:
set entry < 0 | 1> < mac> < ip> < port no> < vid>
Description:
To set ip mac binding entry
Argument:
< 0 | 1> : 0 : Client , 1: Server
<mac> : mac address
< ip > : ip address
< port > : syntax 1,5-7, available from 1 to 16
< vid > : vlan id, 1 to 4094
Possible value:
< 0 | 1> : 0 : Client , 1: Server
<mac> : format: 00-02-03-04-05-06
< ip > : ip address
< port > : 1 to 16
< vid > : 1 to 4094

Example:

GS-2216L(ip_mac_binding)# set entry 1 00-11-2f-de-7b-a9 192.168.2.2 1 1

delete ip

Syntax:
delete ip < 0 | 1> <ip>
Description:
Delete ip mac binding entry by ip.
Argument:
<0 | 1> : 0 : client, 1: server
<ip> : ip address
Possible value:
None
Example:

GS-2216L(ip_mac_binding)# delete ip 1 192.168.2.2

set state

Syntax:
show
Description:
To display the mac alias entry.
Argument:
None
Possible value:
None
Example:
GS-2216L(mac-table-alias)# show
MAC Alias List

	MAC Address	Alias
1)	00-02-03-04-05-06	aaa
2)	00-33-03-04-05-06	ccc
3)	00-44-33-44-55-44	www

■ loop-detection

disable

Syntax:
disable <#>
Description:
To disable switch ports the loop detection function.
Argument:
<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 16
Possible value:
<#> :1 to 24
Example:

GS-2216L(loop-detection)# disable 1-16

GS-2216L(loop-detection)# show

Detection Port Locked Port

Port Status Port Status

---

1 Disable 1 Normal

2 Disable 2 Normal

3 Disable 3 Normal

4 Disable 4 Normal

5 Disable 5 Normal

6 Disable 6 Normal

7 Disable 7 Normal

8 Disable 8 Normal

……

enable

Syntax:
enable <#>
Description:
To enable switch ports the loop detection function.
Argument:
<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to16
Possible value:
<#> :1 to 16
Example:

GS-2216L(loop-detection)# enable 1-16

GS-2216L(loop-detection)# show

Detection Port Locked Port

Port Status Port Status

---

1 Enable 1 Normal

2 Enable 2 Normal

3 Enable 3 Normal

4 Enable 4 Normal

5 Enable 5 Normal

6 Enable 6 Normal

7 Enable 7 Normal

8 Enable 8 Normal

…….

Resume

Syntax:
resume <#>
Description:
To resume locked ports on switch.
Argument:
<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 16
Possible value:
<#> :1 to 16
Example:

GS-2216L (loop-detection)# resume 1-16

GS-2216L (loop-detection)# show

Detection Port Locked Port

Port Status Port Status

---

1 Enable 1 Normal

2 Enable 2 Normal

3 Enable 3 Normal

4 Enable 4 Normal

5 Enable 5 Normal

6 Enable 6 Normal

7 Enable 7 Normal

8 Enable 8 Normal

…….

show

Syntax:
show
Description:
To display loop detection configure.
Argument:
None
Possible value:
None
Example:

GS-2216L (loop-detection)# show

Detection Port Locked Port

Port Status Port Status

```
---------------------------------
  1  Enable        1  Normal
  2  Enable        2  Normal
  3  Enable        3  Normal
  4  Enable        4  Normal
  5  Enable        5  Normal
  6  Enable        6  Normal
  7  Enable        7  Normal
  8  Enable        8  Normal
  ……
```

■ mac-table

<<alias>>

del

Syntax:
del <mac>
Description:
To delete the mac alias entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
Possible value:
<mac> : mac address
Example:
GS-2216L(mac-table-alias)# del 00-44-33-44-55-44

set

Syntax:
set <mac> <alias>
Description:
To set up the mac alias entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<alias> : mac alias name, max. 15 characters
Possible value:
None
Example:
GS-2216L(mac-table-alias)# set 00-44-33-44-55-44 www

show

Syntax:
show
Description:
To display the mac alias entry.
Argument:
None
Possible value:
None
Example:
GS-2216L(mac-table-alias)# show
MAC Alias List
MAC Address Alias
----- ----------------- ----------------
1) 00-02-03-04-05-06 aaa
2) 00-33-03-04-05-06 ccc
3) 00-44-33-44-55-44 www

<<information>>

search

Syntax:
search <port> <mac> <vid>
Description:
To look for the relative mac information in mac table.

Argument:
<port> : set up the range of the ports to search for,
syntax 1,5-7, available form 1 to 16
<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used
<vid> : vlan id, from 1 to 4094; '?' as don't care, 0 as untagged
Possible value:
<port> :1 to 16
<vid> : 0, 1 ~4094
Example:

GS-2216L(mac-table-information)# search 1-16 ??-??-??-??-??-?? ?

MAC Table List

Alias	MAC Address	Port	VID	State
	00-40-c7-88-00-06	1	0	Dynamic

show

Syntax:
show
Description:
To display all mac table information.
Argument:
None
Possible value:
None
Example:

GS-2216L (mac-table-information)# show

MAC Table List

Alias	MAC Address	Port	VID	State
	00-10-db-1d-c5-a0	16	0	Dynamic
	00-40-f4-89-c9-7f	16	0	Dynamic
	00-e0-18-2b-9d-e2	16	0	Dynamic
	00-40-c7-d8-00-02	16	0	Dynamic

<<maintain>>

set aging

Syntax:
set aging <#>
Description:
To set up the age out time of dynamic learning mac.
Argument:
<#>: age-timer in seconds, 0, 10 to 65535. The value “0” means to disable aging
Possible value:
<#>: 0, 10 to 65535.
Example:
GS-2216L(mac-table-maintain)# set aging 300

set flush

Syntax:
set flush
Description:
To delete all of the MACs that is learned dynamically.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(mac-table-maintain)# set flush

show

Syntax:
show
Description:
To display the settings of age-timer.
Argument:
None
Possible value:
None
Example:
GS-2216L(mac-table-maintain)# show
age-timer : 300 seconds
GS-2216L(mac-table-maintain)#

<<static-mac>>

add

Syntax:
add <mac> <port> <vid> [alias]
Description:
To add the static mac entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<port> : 0-16. The value “0” means this entry is filtering entry
<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based
[alias] : mac alias name, max. 15 characters
Possible value:
<mac> : mac address
<port> : 0-16
<vid> : 0, 1-4094
[alias] : mac alias name
Example:
GS-2216L(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 aaa
GS-2216L(mac-table-static-mac)#

del

Syntax:
del <mac> <vid>
Description:
To remove the static mac entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based
Possible value:
<mac> : mac address
<vid> : 0, 1-4094
Example:
GS-2216L(mac-table-static-mac)# del 00-02-03-04-05-06 0
GS-2216L(mac-table-static-mac)#

show filter

Syntax:
show filter
Description:
To display the static filter table.
Argument:
None
Possible value:
None
Example:
GS-2216L(mac-table-static-mac)# show filter
Static Filtering Etnry: (Total 1 item(s))
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
GS-2216L(mac-table-static-mac)#

show forward

Syntax:
show forward
Description:
To display the static forward table.
Argument:
None
Possible value:
None
Example:
GS-2216L(mac-table-static-mac)# show forward
Static Forwarding Etnry: (Total 1 item(s))
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
GS-2216L(mac-table-static-mac)#

■ management

add

Syntax:
Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]
[<type> <value>] <action> <value>
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90
Description:
To save the adding management policy records.
When you don't know how to set the management policy records, you can use this command as follows:

GS-2216L (management-add)# set

This command will show exhaustive operating explanation for setting the management policy records.
Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any.
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any.
<action> <value>	No default and it must be set.

Example:

GS-2216L(management-add)# set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8 type h,s

action a

GS-2216L(management-add)# show

#: 1

Name : Mary VlanID : 20 IP : 192.168.1.1-192.168.1.90

Type : Http,SNMP Action : Accept Port : 2,3,4,5,8

delete

Syntax:
delete #
Description:
To delete a specific record or range.
Argument:
<#>: a specific or range management security entry(s)
Possible value:
None
Example:

```
GS-2216L(management)# show

 #: 1
Name : Tom              VlanID : 2        IP : 192.168.1.30-192.168.1.80
Type : SNMP             Action : Deny     Port : 1,2

GS-2216L(management)# delete 1

GS-2216L(management)# show

Security rule list is empty now
```

edit [#]: the specific management policy entry. Available range: 1 to 65536.

Syntax:
Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]
[<type> <value>] <action> <value>
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90
Description:
To edit management policy record.
Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP Range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any
<action> <value>	No default and it must be set.

Example:

GS-2216L(management)# edit 1

GS-2216L(management-edit-1)# set name Tom vid 2 ip 192.168.1.30-192.168.1.80 port 1-2 type s action d

GS-2216L(management-edit-1)# show

#: 1

Name : Tom VlanID : 2 IP : 192.168.1.30-192.168.1.80

Type : SNMP Action : Deny Port : 1,2

show

Syntax:
show
Description:
To show the specific management policy record.
Argument:
None
Possible value:
None
Example:

GS-2216L(management)# show

#: 1

Name : Tom VlanID : 2 IP : 192.168.1.30-192.168.1.80

Type : SNMP Action : Deny Port : 1,2

■ max-pkt-len

set len

Syntax:
set len <range> <length>
Description:
To set up the maximum length of the packet that each port of the switch can accept. **Argument**:
<range>: port range, syntax 1,5-7, available from 1 to 16
<length (bytes)>: maximum packet length
Possible value:
<range> : 1 to 16
<length (bytes)>: 1518/1532/9216
Example:
GS-2216L(max-pkt-len)# set len 1-8 9216

show

Syntax:
show
Description:
To show current setting of maximum packet length setting.
Argument:
None
Possible value:
None
Example:
GS-2216L(max-pkt-len)# show

PORT	Max Packet Length
1	1532
2	1532
3	1532
4	1532
5	1532
6	1532
7	1532
8	1532
9	1532
10	1532
11	1532
12	1532
13	1532
14	1532
15	1532
16	1532

■ mirror

set mirror-mode

Syntax:
set mirror-mode <rx|disable>
Description:
To set up the mode of mirror (rx mode or disable).
Argument:
<rx | disable>:
rx : enable the mode of mirror(Only mirror the packets that is received)
disable: end the function of mirror
Possible value:
<rx | disable>: rx or disable
Example:
GS-2216L(mirror)# set mirror-mode rx

set monitored-port

Syntax:
set monitored-port <range>
Description:
To set up the port that will be monitored. The packets received by this port will be copied to the monitoring port.
Argument:
<range>: the port that is chosen for monitored port of the mirror function,
syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(mirror)# set monitored-port 3-5,8,10

set monitoring-port

Syntax:
set monitoring-port <#>
Description:
To set up the monitoring port of the mirror function. User can observe the packets that the monitored port received via this port.
Argument:
<#>: the monitoring port that is chosen for the mirror function. Only one port is allowed to configure, available from 1 to 16
Possible value:
<#>:1 to 16
Example:
GS-2216L(mirror)# set monitoring-port 2

show

Syntax:
show
Description:
To display the setting status of Mirror function.

Argument:
None
Possible value:
None
Example:
GS-2216L(mirror)# show
Mirror Mode : rx
Monitoring Port : 2
Monitored Port : 3 4 5 7 10

■ mstp

disable

Syntax:
disable
Description:
To disable mstp function.
Argument:
None
Possible value:
None
Example:
GS-2216L (mstp)# disable

enable

Syntax:
enable
Description:
To enable mstp function.
Argument:
None
Possible value:
None
Example:
GS-2216L (mstp)# enable

migrate-check

Syntax:
migrate-check <port-range>
Description:
To force the port to transmit RST BPDUs.
Argument:
Usage: migrate-check <port range>
port range syntax: 1,5-7, available from 1 to 16
Possible value:
Usage: migrate-check <port range>
port range syntax: 1,5-7, available from 1 to 16
Example:
GS-2216L (mstp)# migrate-check 1-2

set config

Syntax:
set config <Max Age><Forward Delay><Max Hops>
Description:
To set max age,forward delay,max hops.
Argument:
<Max Age> : available from 6 to 40. Recommended value is 20
<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15
<Max Hops> : available from 6 to 40. Recommended value is 20
Possible value:
<Max Age> : available from 6 to 40. Recommended value is 20
<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15

<Max Hops> : available from 6 to 40. Recommended value is 20
Example:

GS-2216L(mstp)# set config 20 15 20

GS-2216L(mstp)#

set msti-vlan

Syntax:
set msti-vlan <instance-id><vid-string>
Description:
To map Vlan ID(s) to an MSTI
Argument:
<instance-id> : MSTI id available from 1 to 4095
<vid-string> : syntax example: 2.5-7.100-200
Possible value:
<instance-id> : available from 1 to 4094
Example:

GS-2216L(mstp)# set msti-vlan 2 2.5

msti 2 had been successfully created and(or)

vlan(s) have been added to map to this msti.

GS-2216L(mstp)#

set p-cost

Syntax:
set p-cost <instance_id> <port range> <path cost>
Description:
To set port path cost per instance
Argument:
<port range> syntax: 1,5-7, available from 1 to 16
<path cost> : 0, 1-200000000. The value zero means auto status
Possible value:
<port range> : available from 1 to 16
<path cost> : The value zero means auto status, 0-2000000000
Example:

GS-2216L(mstp)# set p-cost 2 8-10 0

GS-2216L(mstp)#

set p-edge

Syntax:
set p-edge <port range> <admin edge>
Description:
To set per port admin edge
Argument:
<port range> syntax: 1,5-7, available from 1 to 16
<admin edge> : 0->non-edge port,1->edge ports
Possible value:
<port range> syntax: 1,5-7, available from 1 to 16
<admin edge> : 0->non-edge port,1->edge ports
Example:

GS-2216L(mstp)# set p-edge 10-12 0

GS-2216L(mstp)#

set p-hello

Syntax:
set p-hello <port range> <hello time>
Description:
To set per port hello time
Argument:
<port range> : syntax: 1,5-7, available from 1 to 16
<hello time> : only 1~2 are valid values
Possible value:
<port range> : syntax: 1,5-7, available from 1 to 16
<hello time> : only 1~2 are valid values
Example:

GS-2216L(mstp)# set p-hello 5-10 1

GS-2216L(mstp)#

set p-p2p

Syntax:
set p-p2p <port range> <admin p2p>
Description:
To set per port admin p2p
Argument:
<port range> syntax: 1,5-7, available from 1 to 16
<admin p2p> : Admin point to point, <auto|true|false>
Possible value:
<port range> syntax: 1,5-7, available from 1 to 16
<admin p2p> : Admin point to point, <auto|true|false>
Example:

GS-2216L(mstp)# set p-p2p 8-10 auto

GS-2216L(mstp)#

set priority

Syntax:
set priority <instance-id><Instance Priority>
Description:
To set instance priority
Argument:
<instance-id> : 0->CIST; 1-4095->MSTI
<Instance Priority> : must be a multiple of 4096,available from 0 to 61440
Possible value:
<instance-id> : 0->CIST; 1-4095->MSTI
<Instance Priority> : 0 to 61440
Example:

GS-2216L(mstp)# set priority 0 4096

GS-2216L(mstp)# enable

MSTP started

GS-2216L(mstp)# show instance 0

mstp status : enabled

force version : 3

instance id: 0

bridge max age : 20

bridge forward delay : 15

bridge max hops : 20

instance priority : 4096

bridge mac : 00:40:c7:5e:00:09

CIST ROOT PRIORITY : 4096

CIST ROOT MAC : 00:40:c7:5e:00:09

CIST EXTERNAL ROOT PATH COST : 0

CIST ROOT PORT ID : 0

CIST REGIONAL ROOT PRIORITY : 4096

CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09

CIST INTERNAL ROOT PATH COST : 0

CIST CURRENT MAX AGE : 20

CIST CURRENT FORWARD DELAY : 15

TIME SINCE LAST TOPOLOGY CHANGE(SECs) : 2

TOPOLOGY CHANGE COUNT(SECs) : 0

GS-2216L(mstp)#

set r-role

Syntax:
set r-role <port range> <restricted role>
Description:
To set per port restricted role
Argument:
<port range> syntax: 1,5-7, available from 1 to 16
<restricted role> : 0->false,1->True
Possible value:
<port range> : 1 to 16
<restricted role> : 0->false,1->True
Example:

GS-2216L(mstp)# set r-role 8-12 1

GS-2216L(mstp)# set r-role 13-16 0

GS-2216L(mstp)# show ports 0

==== =========== ====== ========= ===== ===== ==Operational== =Restricted=

Port Port Status Role Path Cost Pri Hello Edge-Port P2P   Role   Tcn

==== =========== ====== ========= ===== ===== ========= ===== ====== =====

 1   FORWARDING DSGN   200000 128   2/2   V

 2   DISCARDING dsbl   2000000 128   2/2   V

```
 3   DISCARDING  dsbl    2000000  128   2/2      V
 4   DISCARDING  dsbl    2000000  128   2/2      V
 5   FORWARDING  DSGN     200000  128   2/2      V       V
 6   DISCARDING  dsbl    2000000  128   2/2      V
 7   FORWARDING  DSGN      20000  128   2/2      V       V
 8   DISCARDING  dsbl    2000000  128   2/2      V            V
 9   DISCARDING  dsbl    2000000  128   2/2      V            V
 10   DISCARDING  dsbl    2000000  128   2/2      V            V
 11   DISCARDING  dsbl    2000000  128   2/2      V            V
 12   DISCARDING  dsbl    2000000  128   2/2      V            V
 13   DISCARDING  dsbl    2000000  128   2/2      V
 14   DISCARDING  dsbl    2000000  128   2/2      V
  ..
GS-2216L(mstp)#
```

set r-tcn

Syntax:
set r-tcn <port range> <restricted tcn>
Description:
To set per port restricted tcn
Argument:
<port range> syntax: 1,5-7, available from 1 to 16
<restricted tcn> : 0->false,1->True
Possible value:
<port range> : 1 to 16
<restricted tcn> : 0->false,1->True
Example:

```
GS-2216L(mstp)# set r-tcn 9-10 1

GS-2216L(mstp)# set r-tcn 14 1

GS-2216L(mstp)# show pconf 0

Port Path Cost Priority Hello Edge-Port   P2P   Role   Tcn
  system              Enter in
==== ========= ======== ===== =========  ===== ====== =====...(q to quit)
  2         0    128     2      true     auto  false false
  3         0    128     2      true     auto  false  true
  4         0    128     2      true     auto  false  true
  5         0    128     2      true     auto  false false
  6         0    128     2      true     auto  false false
  7         0    128     2      true     auto  false false
  8         0    128     2      true     auto   true false
  9         0    128     2      true     auto   true  true
 10         0    128     2      true     auto   true  true
```

11	0	128	2	true	auto	true	false
12	0	128	2	true	auto	true	false
13	0	128	2	true	auto	false	false
14	0	128	2	true	auto	false	true

……

GS-2216L(mstp)#

set region-name

Syntax:
set region-name <string>
Description:
To set mstp region name(0~32 bytes)
Argument:
<string> :a null region name
Possible value:
<string> :1-32
Example:

GS-2216L(mstp)# set region-name test2

GS-2216L(mstp)# show region-info

Name : test2

Revision : 0

Instances : 0

GS-2216L(mstp)#

set revision-level

Syntax:
set rev <revision-level>
Description:
To set mstp revision-level(0~65535)
Argument:
<revision-level> :0~65535
Possible value:
<revision-level> :0~65535
Example:

GS-2216L(mstp)# set revision-level 30000

GS-2216L(mstp)# show region-info

Name : test2

Revision : 30000

Instances : 0

GS-2216L(mstp)#

set version

Syntax:
set version <stp|rstp|mstp>
Description:
To set force-version
Argument:
<revision-level> :0~65535
Possible value:
<revision-level> :0~65535
Example:
GS-2216L(mstp)# set version mstp

show instance

Syntax:
show instance <instance-id>
Description:
To show instance status
Argument:
<instance-id> :0->CIST;1-4095->MSTI
Possible value:
<instance-id> :0->CIST;1-4095->MSTI
Example:
GS-2216L(mstp)# show instance 0

mstp status : enabled

force version : 2

instance id: 0

bridge max age : 20

bridge forward delay : 15

bridge max hops : 20

instance priority : 4096

bridge mac : 00:40:c7:5e:00:09

CIST ROOT PRIORITY : 4096

CIST ROOT MAC : 00:40:c7:5e:00:09

CIST EXTERNAL ROOT PATH COST : 0

CIST ROOT PORT ID : 0

CIST REGIONAL ROOT PRIORITY : 4096

CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09

CIST INTERNAL ROOT PATH COST : 0

CIST CURRENT MAX AGE : 20

CIST CURRENT FORWARD DELAY : 15

TIME SINCE LAST TOPOLOGY CHANGE(SECs) : 2569

TOPOLOGY CHANGE COUNT(SECs) : 0

GS-2216L(mstp)#

show pconf

Syntax:
show pconf <instance-id>
Description:
To show port configuration
Argument:
instance-id:0->CIST;1-4095->MSTI
Possible value:
<instance-id> :0->CIST;1-4095->MSTI
Example:

GS-2216L(mstp)# show pconf 0

set r-role		Se					
2	0	128	2	true	auto	false	false
3	0	128	2	true	auto	false	true
4	0	128	2	true	auto	false	true
5	0	128	2	true	auto	false	false
6	0	128	2	true	auto	false	false
7	0	128	2	true	auto	false	false

…….

12	0	128	2	true	auto	true	false

……

GS-2216L(mstp)#

show ports

Syntax:
show ports <instance-id>
Description:
To show port status
Argument:
instance-id:0->CIST;1-4095->MSTI
Possible value:
<instance-id> :0->CIST;1-4095->MSTI
Example:

GS-2216L(mstp)# show ports 0

show region-info

Syntax:
show region-info
Description:
To show region config
Argument:
none
Possible value:
none
Example:

GS-2216L(mstp)# show region-info

Name : test2

Revision : 30000

Instances : 0

GS-2216L(mstp)#

show vlan-map

Syntax:
show vlan-map <instance-id>
Description:
To show vlan mapping of an instance
Argument:
<nstance-id> :0->CIST;1-4095->MSTI
Possible value:
<instance-id> :0->CIST;1-4095->MSTI
Example:

GS-2216L(mstp)# show vlan-map 0

instance 0 has those vlans :

0-4095

GS-2216L(mstp)#

■ policy

add

Syntax:
add [name <value>] [ip <value>] [port <value>] [type <value>] action <value>
Description:
To add a new management policy entry.
Argument:
Synopsis: add name George ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a
Synopsis: add name Mary ip 192.168.2.1-192.168.2.90 action deny
Possible value:
None
Example:

GS-2216L(policy)# add name Mary ip 192.168.3.1-192.168.3.4 action deny

GS-2216L(policy)# show

1) Name : george IP Range : 192.168.1.1-192.168.1.90

Action : Accept Access Type : HTTP SNMP

Port : 2 3 4 5 8

2) Name : rule1 IP Range : 192.168.2.1-192.168.2.30

Action : Deny Access Type : HTTP TELENT SNMP

Port : 11 12 13 14 15

3) Name : Mary IP Range : 192.168.3.1-192.168.3.4

Action : Deny Access Type : Any

Port : Any

GS-2216L(policy)#

delete

Syntax:
delete <index>
Description:
To add a new management policy entry.
Argument:
<index> : a specific or range management policy entry(s)
e.g. delete 2,3,8-12
Possible value:
<index> : a specific or range management policy entry(s)
Example:

GS-2216L(policy)# add name rule2 ip 192.168.4.23-192.168.4.33 port 6-8 type s,t

action d

GS-2216L(policy)# show

1) Name : rule1 IP Range : 192.168.4.5-192.168.4.22

Action : Deny Access Type : HTTP TELENT SNMP

Port : 2 3 4 5

2) Name : rule2 IP Range : 192.168.4.23-192.168.4.33

Action : Deny Access Type : TELENT SNMP

Port : 6 7 8

GS-2216L(policy)# delete 2

GS-2216L(policy)# show

1) Name : rule1 IP Range : 192.168.4.5-192.168.4.22

Action : Deny Access Type : HTTP TELENT SNMP

Port : 2 3 4 5

GS-2216L(policy)#

show

Syntax:
show
Description:
To show management policy list.
Argument:
none
Possible value:
none
Example:

GS-2216L(policy)# show

1) Name : rule1 IP Range : 192.168.4.5-192.168.4.22

Action : Deny Access Type : HTTP TELENT SNMP

Port : 2 3 4 5

2) Name : rule2 IP Range : 192.168.4.23-192.168.4.33

Action : Deny Access Type : TELENT SNMP

Port : 6 7 8

■ port

clear counter

Syntax:
clear counter
Description:
To clear all ports' counter (include simple and detail port counter) information.
Argument:
None
Possible value:
None
Example:
GS-2216L (port)# clear counter

disable flow-control

Syntax:
disable flow-control <range>
Description:
To disable the flow control function of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 ~ 16
Example:
GS-2216L (port)# disable flow-control 6

disable state

Syntax:
disable state <range>
Description:
To disable the communication capability of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 ~ 16
Example:
GS-2216L (port)# disable state 12

enable flow-control

Syntax:
enable flow-control <range>
Description:
To enable the flow control function of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 ~ 16
Example:
GS-2216L (port)# enable flow-control 3-8

enable state

Syntax:
enable state <range>
Description:
To enable the communication capability of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 ~ 16
Example:
GS-2216L (port)# enable state 3-12

set speed-duplex

Syntax:
set speed-duplex <range> <auto|10half|10full|100half|100full|1Gfull>
Description:
To set up the speed and duplex of all ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 16
<port-speed>:
auto: set auto-negotiation mode
10half: set speed/duplex 10M Half
10full: set speed/duplex 10M Full
100half: set speed/duplex 100M Half
100full: set speed/duplex 100M Full
1Gfull: set speed/duplex 1G Full
Possible value:
<range>: 1 to 16
<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull
Example:
GS-2216L(port)# set speed-duplex 5 auto

show conf

Syntax:
show conf
Description:
To display the each port's configuration about state, speed-duplex and flow control.
Argument:
None.
Possible value:
None.
Example:
GS-2216L (port)# show conf

show detail-counter

Syntax:
show detail-counter <#>
Description:
To display the detailed counting number of each port's traffic.
Argument:
<#>: port, available from 1 to 16
Possible value:
<#>:1 ~ 16
Example:
GS-2216L (port)# show detail-counter 5

show sfp

Syntax:
show sfp <port>
Description:
To display the SFP module information.
Argument:
<port>: SFP port of the switch, available from 13~ 16
Possible value:
<port>: 13, 14, 15, 16
Example:
GS-2216L (port)# show sfp 14

Port 23 SFP information

Connector Type : SFP - LC

Fiber Type : Multi-mode (MM)

Tx Central Wavelength : 850

Baud Rate : 1G

Vendor OUI : 00:40:c7

Vendor Name : APAC Opto

Vendor PN : KM28-C3S-TC-N

Vendor Rev : 0000

Vendor SN : 5425010708

Date Code : 050530

Temperature : none

Vcc : none

Mon1 (Bias) mA : none

Mon2 (TX PWR) : none

Mon3 (RX PWR) : none

show simple-counter

Syntax:
show simple-counter
Description:
To display the summary counting of each port's traffic.
Argument:
None.
Possible value:
None.
Example:
GS-2216L (port)# show simple-counter

show status

Syntax:
show status
Description:
To display the port's current status.
Argument:
None.
Possible value:
None.
Example:
GS-2216L (port)# show status

■ qos

set advance-layer4

Syntax:
set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>
Description:
To set class of ports on advanced mode of Layer 4 qos.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 16
<#>: special UDP/TCP port selection, range: 1-10
<tcp/udp port range>: 0-65535.
<default>: default class (all other TCP/UDP ports). 1: high, 0: low
<match>: special TCP/UDP class. 1: high, 0: low
Possible value:
<port-range>: 1 to 16
<#>: 1-10
<tcp/udp port range>: 0-65535
<default>: 1 or 0
<match>: 1 or 0
Example:
GS-2216L(qos)# set advance-layer4 5 2 80 1 0

set default

Syntax:
set default <class>
Description:
To set priority class of the packets that qos won't affect.
Argument:
<class>: class of service setting. 1: high, 0: low
Possible value:
<class>: 1 or 0
Example:
GS-2216L(qos)# set default 1

set diffserv

Syntax:
set diffserv <ds-range> <class>
Description:
To set class of ports on IP DiffServe qos.
Argument:
<ds-range>: dscp field, syntax 1,5-7, available from 0 to 63
<class>: class of service setting. 1: high, 0: low
Possible value:
<ds-range>: 0 to 63
<class>: 1or 0
Example:
GS-2216L(qos)# set diffserv 0-20 1

set mode

Syntax:
set mode <port/pri_tag/tos/layer4/diffserv>
Description:
To set qos priority mode of the switch.
Argument:
<port>: per port priority
<pri_tag>: vlan tag priority
<tos>: ip tos classification
<layer4>: ip tcp/udp port classification
<diffserv>: ip diffserv classification
Possible value:
port/pri_tag/tos/layer4/diffserv
Example:

GS-2216L(qos)# set mode port

set port

Syntax:
set port <range> <class>
Description:
To set class of ports on port-based qos.
Argument:
<range> : port range, syntax 1,5-7, available from 1 to 16
<class> : class of service setting. 1: high, 0: low
Possible value:
<range>: 1 to 16
<class>: 1or 0
Example:

GS-2216L(qos)# set port 1-10 1

set pri-tag

Syntax:
set pri_tag <port-range> <tag-range> <class>
Description:
To set class of ports on vlan tag-based qos.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 16
<tag-range>: tag priority level, syntax: 1,5-7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low
Possible value:
<port-range>: 1 to 16
<tag-range>: 0 to 7
<class>: 1or 0
Example:
GS-2216L(qos)# set pri-tag 1-15 1-2 1

set simple-layer4

Syntax:
set simple-layer4 <#>
Description:
To set class of ports on simple mode of Layer 4 qos.
Argument:
<#>: layer-4 configuration mode, valid values are as follows:
0: disable ip tcp/udp port classification
1: down prioritize web browsing, e-mail, FTP and news
2: prioritize ip telephony (VoIP)
3: prioritize iSCSI
4: prioritize web browsing, e-mail, FTP transfers and news
5: prioritize streaming Audio/Video
6: prioritize databases (Oracle, IBM DB2, SQL, Microsoft)
Possible value:
<#>:0~6
Example:
GS-2216L(qos)# set simple-layer4 2

set tos

Syntax:
set tos <port-range> <tos-range> <class>
Description:
To set class of ports on IP TOS qos.
Argument:
<port-range>: port range, syntax: 1,5-7, available from 1 to 16
<tos-range>: tos precedence field, syntax 1,5-7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low
Possible value:
<port-range>: 1 to 16
<tos-range>: 0 to 7
<class>: 1or 0
Example:

GS-2216L(qos)# set tos 1-5 0-3 0

show

Syntax:
show
Description:
To display the information of the mode you choose.
Argument:
None.
Possible value:
None.
Example:

GS-2216L (qos)# show

IP Diffserv Classification

Default Class:high

DiffServ	Class	DiffServ	Class	DiffServ	Class	DiffServ	Class
0	high	1	high	2	high	3	high
4	high	5	high	6	high	7	high
8	high	9	high	10	high	11	high
12	high	13	high	14	high	15	high
16	high	17	high	18	high	19	high
20	high	21	high	22	high	23	high
24	high	25	high	26	high	27	high
28	high	29	high	30	high	31	high
32	high	33	high	34	high	35	high
36	high	37	high	38	high	39	high
40	high	41	high	42	high	43	high
44	high	45	high	46	high	47	high
48	high	49	high	50	high	51	high
52	high	53	high	54	high	55	high
56	high	57	high	58	high	59	high

60 high 61 high 62 high 63 high

■ reboot

reboot

Syntax:
reboot
Description:
To reboot the system.
Argument:
None.
Possible value:
None.
Example:
GS-2216L# reboot

■ snmp

disable

Syntax:
disable set-ability
disable snmp
Description:
The Disable here is used for the de-activation of snmp or set-community.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(snmp)# disable snmp

GS-2216L(snmp)# disable set-ability

enable

Syntax:
enable set-ability
enable snmp
Description:
The Enable here is used for the activation snmp or set-community.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(snmp)# enable snmp

GS-2216L(snmp)# enable set-ability

set

Syntax:
set get-community <community>
set set-community <community>
set trap <#> <ip> [port] [community]
Description:
The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap-community.
Argument:
<#>: trap number
<ip>: ip address or domain name
<port>: trap port
<community>:trap community name
Possible value:
<#>: 1 to 6
<port>:1~65535
Example:

GS-2216L(snmp)# set get-community public

GS-2216L(snmp)# set set-community private

GS-2216L(snmp)# set trap 1 192.168.1.1 162 public

show

Syntax:
show
Description:
The Show here is to display the configuration of SNMP.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(snmp)# show

SNMP : Enable

Get Community: public

Set Community: private [Enable]

Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public

Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public

■ stp

MCheck

Syntax:
MCheck <range>
Description:
To force the port to transmit RST BPDUs.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(stp)# Mcheck 1-8

disable

Syntax:
disable
Description:
To disable the STP function.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(stp)# disable

enable

Syntax:
enable
Description:
To enable the STP function.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(stp)# enable

set config

Syntax:
set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>
Description:
To set up the parameters of STP.
Argument:
<Bridge Priority>:priority must be a multiple of 4096, available from 0 to 61440.
<Hello Time>: available from 1 to 10.
<Max. Age>: available from 6 to 40.
<Forward Delay>: available from 4 to 30.
Note: 2*(Forward Delay -1) >= Max Age
Max Age >= 2*(Hello Time +1)
Possible value:
<Bridge Priority>: 0 to 61440
<Hello Time>: 1 to 10
<Max. Age>: 6 to 40
<Forward Delay>: 4 to 30
Example:
GS-2216L(stp)# set config 61440 2 20 15

set port

Syntax:
set port <range> <path cost> <priority> <edge_port> <admin p2p>
Description:
To set up the port information of STP.
Argument:
<range>: syntax 1,5-7, available from 1 to 16
<path cost>: 0, 1-200000000. The value zero means auto status
<priority>: priority must be a multiple of 16, available from 0 to 240
<edge_port> : Admin Edge Port, <yes|no>
<admin p2p>: Admin point to point, <auto|true|false>
Possible value:
<range>:1 to 16
<path cost>: 0, 1-200000000
<priority>: 0 to 240
<edge_port>: yes / no
<admin p2p>: auto / true / false
Example:
GS-2216L(stp)# set port 1-16 0 128 yes auto

set version

Syntax:
set version <stp|rstp>
Description:
To set up the version of STP.
Argument:
<stp|rstp>:stp / rstp
Possible value:
<stp|rstp>:stp / rstp
Example:
GS-2216L(stp)# set version rstp

show config

Syntax:
show config
Description:
To display the configuration of STP.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(stp)# show config

STP State Configuration :

Spanning Tree Protocol : Enabled

Bridge Priority (0-61440) : 61440

Hello Time (1-10 sec) : 2

Max. Age (6-40 sec) : 20

Forward Delay (4-30 sec) : 15

Force Version : RSTP

show port

Syntax:
show port
Description:
To display the port information of STP.
Argument:
None.
Possible value:
None.
Example:

GS-2216L# stp

GS-2216L(stp)# show port

Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point

==== ========== ========= ======== ============== ==================

1	DISCARDING	2000000	128	No	Auto
2	DISCARDING	2000000	128	No	Auto
3	DISCARDING	2000000	128	No	Auto
4	DISCARDING	2000000	128	No	Auto
5	DISCARDING	2000000	128	No	Auto
6	DISCARDING	2000000	128	No	Auto
7	DISCARDING	2000000	128	No	Auto
8	DISCARDING	2000000	128	No	Auto
9	DISCARDING	2000000	128	No	Auto
10	DISCARDING	2000000	128	No	Auto
11	DISCARDING	2000000	128	No	Auto
12	DISCARDING	2000000	128	No	Auto
13	DISCARDING	2000000	128	No	Auto
14	DISCARDING	2000000	128	No	Auto
15	DISCARDING	2000000	128	No	Auto
16	DISCARDING	2000000	128	No	Auto

show status

Syntax:
show status
Description:
To display the status of STP.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(stp)# show status

STP Status :

STP State : Enabled

Bridge ID : 00:40:C7:D8:09:1D

Bridge Priority : 61440

Designated Root : 00:40:C7:D8:09:1D

Designated Priority : 61440

Root Port : 0

Root Path Cost : 0

Current Max. Age(sec) : 20

Current Forward Delay(sec) : 15

Hello Time(sec) : 2

STP Topology Change Count : 0

Time Since Last Topology Change(sec) : 848

■ system

set contact

Syntax:
set contact <contact string>
Description:
To set the contact description of the switch.
Argument:
<contact>:string length up to 40 characters.
Possible value:
<contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
GS-2216L(system)# set contact Taipei

set device-name

Syntax:
set device-name <device-name string>
Description:
To set the device name description of the switch.
Argument:
<device-name>: string length up to 40 characters.
Possible value:
<device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
GS-2216L(system)# set device-name CR-2600

set location

Syntax:
set location <location string>
Description:
To set the location description of the switch.
Argument:
<location>: string length up to 40 characters.
Possible value:
<location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
GS-2216L(system)# set location Taipei

show

Syntax:
show
Description:
To display the basic information of the switch.
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(system)# show
Model Name                  : GS-2216L
System Description          : L2 Managed Switch
Location                    :
Contact                     :
Device Name                 : GS-2216L
System Up Time              : 0 Days 0 Hours 4 Mins 14 Secs
Current Time                : Tue Jan 17 16:28:46 2006
BIOS Version                : v1.05
Firmware Version            : v2.08
Hardware-Mechanical Version  : v1.01-v1.01
Serial Number               : 030C02000003
Host IP Address             : 192.168.1.1
Host MAC Address            : 00-40-c7-e7-00-10
Device Port                 : UART * 1, TP * 22, Dual-Media Port(RJ45/SFP) * 2
RAM Size                    : 16 M
Flash Size                  : 2 M
```

■ traplog

clear

Syntax:
clear
Description:
To clear trap log.
Argument:
none
Possible value:
none
Example:

GS-2216L(traplog)# clear

GS-2216L(traplog)# show

No time desc

---- --------------------------- -----------------------------------

show

Syntax:
show
Description:
To display the trap log.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(tftp)# show

2 Mon Mar 17 15:18:38 2008gvrp mode> <qce type> .

Dual Media Swapped [Port:1][SwapTo:TP]ge hostnamexit / 4 / 8

3 Mon Mar 17 15:18:38 2008nto igmp mode, available from

Link Up [Port:1]Enter into ip mode

6 Mon Mar 17 15:18:38 2008

Dual Media Swapped [Port:5][SwapTo:TP]

7 Mon Mar 17 15:18:38 2008

Link Up [Port:5]

8 Mon Mar 17 15:18:48 2008

Login [admin]

■ tftp

set server

Syntax:
set server <ip>
Description:
To set up the IP address of tftp server.
Argument:
<ip>: the IP address of tftp server
Possible value:
<ip>: tftp server ip
Example:
GS-2216L(tftp)# set server 192.168.3.111

show

Syntax:
show
Description:
To display the information of tftp server.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(tftp)# show
Tftp Server : 192.168.3.111

■ time

set daylightsaving

Syntax:
set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>
Description:
To set up the daylight saving.
Argument:
hr : daylight saving hour, range: -5 to +5

MM : daylight saving start Month (01-12)

DD : daylight saving start Day (01-31)

HH : daylight saving start Hour (00-23)

mm : daylight saving end Month (01-12)

dd : daylight saving end Day (01-31)

hh : daylight saving end Hour (00-23)
Possible value:
hr : -5 to +5

MM : (01-12)

DD : (01-31)

HH : (00-23)

mm : (01-12)

dd : (01-31)

hh : (00-23)
Example:
GS-2216L(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully

set manual

Syntax:
set manual <YYYY/MM/DD> <hh:mm:ss>
Description:
To set up the current time manually.
Argument:
YYYY : Year (2000-2036) MM : Month (01-12)

DD : Day (01-31) hh : Hour (00-23)

mm : Minute (00-59) ss : Second (00-59)
Possible value:
YYYY : (2000-2036) MM : (01-12)

DD : (01-31) hh : (00-23)

mm : (00-59) ss : (00-59)
Example:
GS-2216L(time)# set manual 2004/12/23 16:18:00

set ntp

Syntax:
set ntp <ip> <timezone>
Description:
To set up the current time via NTP server.
Argument:
<ip>: ntp server ip address or domain name
<timezone>: time zone (GMT), range: -12 to +13
Possible value:
<timezone>: -12,-11…,0,1…,13
Example:
GS-2216L(time)# set ntp clock.via.net 8
Synchronizing...(1)
Synchronization success

show

Syntax:
show
Description:
To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”, ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”
Argument:
None.
Possible value:
None.
Example:

```
GS-2216L(time)# show

Current Time                : Thu Thu 14 15:04:03 2005
NTP Server                  : 209.81.9.7
Timezone                    : GMT+8:00
Day light Saving            : 0 Hours
Day light Saving Start      : Mth: 1 Day: 1 Hour: 0
Day light Saving End        : Mth: 1 Day: 1 Hour: 0
GS-2216L(time)#
```

■ trunk

del trunk

Syntax:
del trunk <port-range>
Description:
To delete the trunking port.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 16
Possible value:
<port-range>: 1 to 16
Example:
GS-2216L(trunk)# del trunk 1

set priority

Syntax:
set priority <range>
Description:
To set up the LACP system priority.
Argument:
<range>: available from 1 to 65535.
Possible value:
<range>: 1 to 65535, default: 32768
Example:
GS-2216L(trunk)# set priority 33333

set trunk

Syntax:
set trunk <port-range> <method> <group> <active LACP>
Description:
To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.
Argument:
<port-range> : port range, syntax 1,5-7, available from 1 to 16
<method>:
static : adopt the static link aggregation
lacp : adopt the dynamic link aggregation- link aggregation control protocol
<group>: 1-8.
<active LACP>:
active : set the LACP to active mode
passive : set the LACP to passive mode
Possible value:
<port-range> : 1 to 16
<method>: static / lacp
<group>: 1-8.
<active LACP>: active / passive
Example:
GS-2216L(trunk)# set trunk 1-4 lacp 1 active

show aggtr-view

Syntax:
show aggtr-view
Description:
To display the aggregator list.
Argument:

None.
Possible value:
None.
Example:
GS-2216L(trunk)# show aggtr-view
Aggregator 1) Method: None
Member Ports: 1
Ready Ports:1

Aggregator 2) Method: LACP
Member Ports: 2
Ready Ports:
:
:
:

show lacp-detail

Syntax:
show lacp-detail <aggtr>
Description:
To display the detailed information of the LACP trunk group.
Argument:
<aggtr>: aggregator, available from 1 to 16
Possible value:
<aggtr>: 1 to 16
Example:

GS-2216L(trunk)# show lacp-detail 2

Aggregator 2 Information:

Actor		Partner	
System Priority	MAC Address	System Priority	MAC Address
32768	00-40-c7-e8-00-02	32768	00-00-00-00-00-00

Port	Key	Trunk Status	Port	Key
2	257	---	2	0

show lacp-priority

Syntax:
show lacp-priority
Description:
To display the value of LACP Priority.
Argument:
None.
Possible value:
None.

Example:
GS-2216L(trunk)# show lacp-priority
LACP System Priority : 32768

show status

Syntax:
show status
Description:
To display the aggregator status and the settings of each port.
Argument:
None.
Possible value:
None.
Example:
GS-2216L(trunk)# show status

Trunk Port Setting				Trunk Port Status	
port	Method	Group	Active LACP	Aggtregator	Status
1	None	0	Active	1	Ready
2	LACP	1	Active	2	---
3	LACP	1	Active	3	---
4	LACP	1	Active	4	---
5	LACP	1	Active	5	---
6	LACP	1	Active	6	---
7	LACP	1	Active	7	---
		:			
			:		

■ vlan

del port-group

Syntax:
del port-group <name>
Description:
To delete the port-based vlan group.
Argument:
<name>: which vlan group you want to delete.
Possible value:
<name>: port-vlan name
Example:
GS-2216L(vlan)# del port-group VLAN-2

del tag-group

Syntax:
del tag-group <vid>
Description:
To delete the tag-based vlan group.
Argument:
<vid>: which vlan group you want to delete, available from 1 to 4094
Possible value:
<vid>: 1 to 4094
Example:
GS-2216L(vlan)# del tag-group 2

disable drop-untag

Syntax:
disable drop-untag <range>
Description:
Don’t drop the untagged frames.
Argument:
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(vlan)# disable drop-untag 5-10

disable sym-vlan

Syntax:
disable sym-vlan <range>
Description:
To drop frames from the non-member port.
Argument:
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(vlan)# disable sym-vlan 5-10

enable drop-untag

Syntax:
enable drop-untag <range>
Description:
To drop the untagged frames.
Argument:
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(vlan)# enable drop-untag 5-10

enable sym-vlan

Syntax:
enable sym-vlan <range>
Description:
To drop frames from the non-member port.
Argument:
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(vlan)# enable sym-vlan 5-10

set mode

Syntax:
set mode <disable|port|tag|metro|double-tag> [up-link]
Description:
To switch VLAN mode, including disable, port-based, tag-based, metro and double-tag modes.
Argument:
<disable>: vlan disable
<tag>: set tag-based vlan
<port>: set port-based vlan
<metro>: set metro mode vlan
<double-tag>: enable Q-in-Q function
<up-link>: syntax 1,5-7, available from 13 to 16, only for metro mode vlan
Possible value:
<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag
[up-link]: 13, 14, 15 or 16 or “13,16”
Example:
GS-2216L(vlan)# set mode port

set port-group

Syntax:
set port-group <name> <range>
Description:
To add or edit a port-based VLAN group.
Argument:
<name>: port-vlan name
<range>: syntax 1,5-7, available from 1 to 16
Possible value:
<range>: 1 to 16
Example:
GS-2216L(vlan)# set port-group VLAN-1 2-5,6,15-13

set port-role

Syntax:
set port-role <range> <access|trunk|hybrid> [vid]
Description:
To set egress rule: configure the port roles.
Argument:
<range> :which port(s) you want to set, syntax 1,5-7, available from 1 to 16
<access>: Do not tag frames
<trunk>: Tag all frames
<hybrid>: Tag all frames except a specific VID
<vid>: untag-vid for hybrid port
Possible value:
<range>: 1 to 16
<vid>: 1 to 4094
Example:
GS-2216L(vlan)# set port-role 5 hybrid 6

set pvid

Syntax:
set pvid <range> <pvid>
Description:
To set the pvid of vlan.
Argument:
<range>: which port(s) you want to set PVID(s), syntax 1,5-7, available from 1 to 16
<pvid>: which PVID(s) you want to set, available from 1 to 4094
Possible value:
<range>: 1 to 16
<pvid>: 1 to 4094
Example:
GS-2216L(vlan)# set pvid 3,5,6-8 5

set tag-group

Syntax:
set tag-group <vid> <name> <range> <#>
Description:
To add or edit the tag-based vlan group.
Argument:
<vid>: vlan ID, range from 1 to 4094
<name>: tag-vlan name
<range>: vlan group members, syntax 1,5-7, available from 1 to 16
<#>: sym/asym vlan setting. 1: symmetric vlan, 0: asymmetric vlan
Possible value:
<vid>: 1 to 4094
<range>: 1 to 16
<#>: 0 or 1
Example:
GS-2216L(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0

show group

Syntax:
show group
Description:
To display the vlan mode and vlan group.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(vlan)# show group

Vlan mode is double-tag.

1) Vlan Name : default

Vlan ID : 1

Sym-vlan : Disable

Member : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2) Vlan Name : VLAN-2

Vlan ID : 2

Sym-vlan : Disable

Member : 2 3 4 5 6 13 14 15

show pvid

Syntax:
show pvid
Description:
To display pvid, ingress/egress rule.
Argument:
None.
Possible value:
None.
Example:

GS-2216L(vlan)# show pvid

Port	PVID	Rule1	Rule2	Port Rule	Untag Vid
1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-
9	1	Enable	Disable	Access	-
10	1	Enable	Disable	Access	-
11	1	Disable	Disable	Access	-
:					
				:	

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.
   - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
   - ✓ The network configuration of Computer C may be wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ Please check if connection ports are used on that Managed Switch.
   - ✓ Please check the uplink setup of the Managed Switch to verify the uplink function is enabled.

3. The console interface does not appear on the console port connection.
   - ✓ The COM port default parameters are [Baud Rate: 115200, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None]. Please check the COM port properties in the terminal program. And if the parameters are changed, please set the COM configuration to the new setting.
   - ✓ Check the RS-232 cable is connected properley on the console port of the Managed Switch and COM port of PC.
   - ✓ Check if the COM of the PC is enabled.

4. How to configure the Managed Switch?
   - ✓ The “Hyperterm” is the terminal program in Win95/98/NT. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Please refer to the user guide of that terminal program. But the COM port parameters (baud rate/ data bits/ parity bits/ flow control) must be the same as the setting of the console port of the Managed Switch.

Appendix A
Technical Specifications

Features

- 12 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 4 Gigabit TP/SFP fiber are dual media ports with auto detect function.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any port can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of range from 1518 to 9600 bytes jumbo frame.
- Supports port-based VLAN, 802.1Q tag-based VLAN.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.
- Web-based management provides the ability to completely manage the switch from any web browser.
- SNMP/Telnet interface delivers complete in-band management.
- Supports IEEE 802.1d Spanning Tree Protocol.
- Supports IEEE 802.1w Rapid Spanning Trees.
- Supports IEEE 802.1s Multiple Spanning Trees.
- Supports IEEE 802.1X port-based network access control.
- Supports ACL to classify the ingress packets to do permit/deny, rate limit actions
- Supports QCL to classify the ingress packets for priority queues assignment
- Supports IP-MAC Binding function to prevent spoofing attack
- Supports IP Multicasting to implement IGMP Snooping function.
- Supports 802.1p Class of Service with 4-level priority queuing.
- Supports 802.3ad port trunking with flexible load distribution and failover function.
- Supports ingress port security mode for VLAN Tagged and Untagged frame process.
- Supports SNMP MIB2 and RMON sampling with sampled packet error indication.

Hardware Specifications

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x
- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 16
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	13 to 16(Option)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	13 to 16(Option)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	13 to 16(Option)

*Port 13 to 16 are TP/SFP fiber dual media ports with auto detected function
*Optional SFP module supports LC or BiDi LC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP
  1000Mbps for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning:** 8K MAC address
  4K VLAN table entries,
- **Buffer Memory:** Embedded 816 KB frame buffer
- **Flow Control:** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex
- **Cable and Maximum Length:**

TP	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, up to10/30/50Km
1000Base-LX WDM (BiDi)	Single-Mode Single Fiber, up to 20Km

- **Diagnostic LED:**

  System LED : Power
  Per Port LED:
  10/100/1000M TP Port 1 to 16 : LINK/ACT, 10/100/1000Mbps
  1000M SFP Fiber Port 13 to 16 : SFP(LINK/ACT)

- **Power Requirement** **:** AC Line

  Voltage : 100~240 V
  Frequency : 50~60 Hz
  Consumption : 30W
- **Ambient Temperature** **:** 0° to 40°C
- **Humidity** **:** 5% to 90%
- **Dimensions** **:** 1.73(H) × 17.40(W) × 8.23(D) in
- **Comply with FCC Part 15 Class A & CE Mark Approval**

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100/1000 Base-TX ports, Web browser or console interface can set transmission speed (10/100/1000Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
Management Agent	SNMP support; MIB II, Bridge MIB, RMON MIB
Spanning Tree Algorithm	IEEE 802.1D
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 256 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
IGMP	IP Multicast Filtering by passively snooping on the IGMP Query.
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred to as Class of Service (CoS) by the IEEE 802.1P standard ,Classification of packet priority can be based on either a VLAN tag on packet or a user-defined Per port QoS. Two queues per port IP TOS Classification TCP/UDP Port Classification IP DiffServe Classification
Port Security	Limit number of MAC addresses learned per port static MAC addresses stay in the filtering table.
Internetworking Protocol	Bridging : 802.1D Spanning Tree IP Multicast : IGMP Snooping IP Multicast Packet Filtering Maximum of 256 active VLANs and IP multicast sessions
Network Management	One RS-232 port as local control console Telnet remote control console SNMP agent : MIB-2 (RFC 1213) Bridge MIB (RFC 1493) RMON MIB (RFC 1757)-statistics Ethernet-like MIB (RFC 1643) Web browser support based on HTTP Server and CGI parser TFTP software-upgrade capability.

Note: Any specification is subject to change without notice.

Appendix B
Null Modem Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RS-232 port to access the command-line interface.

The table below shows the pin assignments for the DB-9 cable.

Function	Mnemonic	Pin
Carrier	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

9 Pin Null Modem Cable